

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص إدارة المخاطر



عنوان البحث

تطوير إطار منهجي استباقي لإدارة المخاطر الرقمية الناشئة وأثره على
استدامة التحول الرقمي في الجهات الحكومية السعودية
(الرياض)

إعداد الطالب/ أمانى سعيد الضويلع.

إشراف/

الدكتور: الفيصل عبد الحميد محمد حسن

الدكتور: فايز جراد

العام الدراسي: 2025

الاهداء

أهدي هذا البحث إلى والدتي الكريمة، اللذين كان دعمهما المتواصل وتشجيعهما الدائم مصدر إلهام لي طوال مسيرة التعليم.

إلى أسرتي العزيزة، التي كانت صبورة وداعمة، وساهمت في تهيئة البيئة المناسبة لإكمال هذا العمل.

إلى أساتذتي الأفاضل، الذين أمدوني بالمعرفة والإرشاد، وكانوا قدوة في الاجتهاد والتميز الأكاديمي.

إلى زميلي وصديقي فيصل العمر، الذي شاركني الجهد والصبر وساهم في إنجاح مراحل البحث.

إلى جميع الزملاء والأصدقاء الذين ساهموا بالنقاش العلمي والملاحظات البناءة، مما أثرى هذا البحث.

أهدي هذا العمل لكل من ساهم في تعليمي وإعدادي العلمي، من مشرفين ومرشدين وداعمين.

ليكن هذا البحث تعبيراً عن الامتنان والتقدير لكل من ساهم في مسيرتي الأكاديمية وساعدني على الوصول إلى هذه المرحلة.

شكر وتقدير

أتقدم بخالص الشكر وعظيم الامتنان إلى المولى عز وجل على ما أنعم به عليّ من قوة وعزيمة لإنجاز هذا البحث.

كما أتقدم بجزيل الشكر والتقدير إلى الأستاذين المشرفين الفاضلين:

- الدكتور/ الفیصل عبد الحمید محمد حسن
- الدكتور/ فايز جراد

على توجيهاتهما القيمة، وإشرافهما الحكيم، ودعمهما المستمر الذي كان له الأثر الأكبر في إثراء البحث وإخراجه بهذا الشكل.

وإلى زميلي الفاضل فيصل العمر: أشكرك جزيل الشكر على دعمك ومساندتك المستمرة، والمراجعات المثمرة، والملاحظات البناءة التي أسهمت في تذليل العديد من الصعوبات.

وأخيراً، أتوجه بالشكر لكل من قدم لي العون والمساعدة من قيادات ومختصي الجهات الحكومية لتعاونهم في جمع البيانات وإنجاح هذا العمل البحثي.

حقوق الطبع والنشر

جميع حقوق الطبع والنشر لهذا البحث محفوظة لجامعة ميد أوشن. كافة المواد والمحتويات الواردة في هذا البحث، بما في ذلك النصوص، الجداول، الرسوم التوضيحية، والبيانات التحليلية، هي ملك حصري للجامعة. لا يجوز نسخ، نشر، إعادة نشر، توزيع، أو استخدام أي جزء من محتويات البحث بأي شكل من الأشكال دون الحصول على إذن كتابي مسبق من جامعة ميد أوشن. تُعتبر أي محاولة لاستخدام محتويات البحث دون إذن مسبق انتهاكًا صريحًا لحقوق الملكية الفكرية والقوانين المعمول بها. تهدف هذه الحماية إلى ضمان احترام حقوق المؤلفين والحفاظ على جودة البحث الأكاديمية، ومنع الاستغلال التجاري أو الأكاديمي غير المصرح به. كما تُشجع الجامعة الباحثين والمختصين على الاستفادة العلمية من محتوى البحث ضمن حدود الاستخدام الأكاديمي والاقتباس المصرح به مع ذكر المصدر بشكل صحيح.

المستخلص

هدف الدراسة: تهدف هذه الدراسة إلى تطوير إطار منهجي استباقي مقترح لإدارة المخاطر الرقمية الناشئة، وتحليل مدى تأثير نضج ممارسات إدارة المخاطر الرقمية على نجاح واستدامة مشاريع التحول الرقمي في الجهات الحكومية بالمملكة العربية السعودية، وذلك لسد الفجوة المنهجية في التعامل مع المخاطر المعقدة الناتجة عن التقنيات المتقدمة (كالذكاء الاصطناعي وحوكمة البيانات).

المنهجية: اعتمدت الدراسة على المنهج المختلط (الكمي والنوعي).

1. **الجانب الكمي:** تم استخدام المنهج الوصفي التحليلي من خلال الاستبانة لجمع البيانات من القيادات والمختصين في إدارات المخاطر والأمن السيبراني وتقنية المعلومات بالجهات الحكومية، واختبار الفرضيات المتعلقة بالعلاقة والأثر.
2. **الجانب النوعي:** تم استخدام المنهج الكيفي من خلال المقابلات المتعمقة مع عينة هادفة من الخبراء لاستكشاف المخاطر الناشئة وتفسير النتائج، وتطوير الإطار المنهجى المقترح.

أبرز النتائج المتوقعة: يتوقع أن تتوصل الدراسة إلى وجود علاقة ارتباط موجبة وذات دلالة إحصائية بين نضج أبعاد الإدارة الاستباقية للمخاطر الرقمية (كفاءة الكوادر، وضوح السياسات، وحوكمة البيانات) وبين نجاح واستدامة مبادرات التحول الرقمي في القطاع الحكومي، مما يؤكد أن الاستثمار في إدارة المخاطر يعدّ عاملاً حاسماً في تحقيق مستهدفات رؤية 2030.

أهم التوصيات المتوقعة: تقديم إطار منهجي استباقي يتميز بالمرونة وقابلية المواءمة مع البيئة الحكومية السعودية، يركز على توقع المخاطر الناشئة وتعزيز القدرة المؤسسية على المرونة الرقمية والتعافي.

قائمة المحتويات

الصفحة	المحتوى
1	صفحة العنوان
2	الإهداء
3	الشكر والتقدير
4	حقوق الطبع والنشر
5	المستخلص (ملخص الدراسة)
6	قائمة المحتويات
10	قائمة الجداول
11	قائمة الأشكال والملاحق
14	المقدمة
---	---
15	الفصل الأول: الإطار العام للدراسة
16	1.1 مقدمة
17	1.2 مشكلة الدراسة
20	1.3 أهداف الدراسة

المحتوى	الصفحة
1.4 أهمية الدراسة (العلمية والتطبيقية)	19
1.5 تساؤلات الدراسة	21
1.6 فروض الدراسة	22
1.7 حدود الدراسة (الموضوعية والمكانية والزمانية)	23
1.8 مصطلحات الدراسة الرئيسية	12
---	---
الفصل الثاني: الإطار النظري والدراسات السابقة	26
2.1 مقدمة	27
2.2 الإطار النظري للمتغير المستقل: إدارة المخاطر الرقمية الناشئة	28
2.3 الإطار النظري للمتغير التابع: التحول الرقمي والاستدامة	29
2.4 النظريات التي استندت إليها الدراسة (ERM, Maturity Model, IT Governance)	28
2.5 الدراسات السابقة المتعلقة بموضوع البحث	32
2.6 التعقيب على الدراسات السابقة وتحديد الفجوة البحثية	35
---	---
الفصل الثالث: منهجية الدراسة وإجراءاتها	37
3.1 مقدمة	38

المحتوى	الصفحة
3.2 منهج الدراسة	39
3.3 مجتمع وعينة الدراسة	
3.4 أدوات جمع البيانات (الاستبانة والمقابلات)	38
3.5 صدق وثبات أدوات الدراسة	40
3.6 الأساليب الإحصائية المستخدمة في تحليل البيانات	41
---	---
الفصل الرابع: تحليل وعرض النتائج	54
4.1 مقدمة	55
4.2 تحليل البيانات الوصفية والنتائج التشخيصية (التساؤل الأول والثاني)	56
4.3 اختبار الفرضيات الإحصائية (التساؤل الثالث)	
4.4 نتائج المقابلات المتعمقة (الجزء النوعي)	55
4.5 مناقشة النتائج	56
---	---
الفصل الخامس: الإطار المقترح والتوصيات والخاتمة	60
5.1 مقدمة	61
5.2 الإطار المنهجي الاستباقي المقترح (التساؤل الرابع)	62
5.3 النتائج والتوصيات النهائية للدراسة	65

الصفحة	المحتوى
70	5.4 مقترحات لدراسات مستقبلية
72	المراجع
73	الملاحق

قائمة الجدول

1+	توزيع أفراد العينة
1-2 2+	اختبار الثبات الداخلي
2-1 3+	المتوسطات لبعء وضوح السياسات
2-2 4+	المتوسطات لبعء كفاءة الكوادر
2-3 5+	المتوسطات لبعء الحوكمة الرقمية
2-4 6+	المتوسطات لبعء الوعي المؤسسي
2-5 7+	نضج حوكمة البيانات
2-6 8+	أبرز المخاطر الرقمية
3-1 9+	مؤشرات النجاح والاستدامة
4-1 10+	أثر وضوح السياسات على النضج
4-2 11+	أثر الكوادر على النضج
4-3 12+	أثر الحوكمة على المخاطر التشغيلية
4-4 13+	أثر الوعي على الاستدامة
4-5 14+	أثر حوكمة البيانات على تقييم المخاطر
4-6 ANOVA 15+	للفروق حسب المتغيرات
5-1 16+	تقييم الخبراء للإطار المقترح

فهرس الملاحق

رقم الملحق	عنوان الملحق	الصفحة
ملحق (1)	قائمة بأسماء السادة المحكمين (الأكاديميين والخبراء)	75
ملحق (2)	نموذج الاستبانة في صورتها النهائية المعتمدة للتطبيق	76
ملحق (3)	دليل المقابلة المتعمقة مع الخبراء في إدارة المخاطر الرقمية والأمن السيبراني	82
ملحق (4)	خطاب التسهيل الرسمي الموجه للجهات الحكومية لجمع البيانات	85
ملحق (5)	النتائج التفصيلية لاختبار الثبات (Cronbach's Alpha) لأبعاد الاستبانة	86
ملحق (6)	محضر تحكيم الإطار المنهجي الاستباقي المقترح	88
ملحق (7)	قائمة بأسماء الخبراء الذين شاركوا في المقابلات (العينة الهادفة)	90

مصطلحات البحث

المصطلح	التعريف النظري	التعريف الإجرائي في البحث
1. التحول الرقمي (Digital Transformation)	استخدام التقنيات الرقمية لإحداث تغييرات جوهرية في نماذج الأعمال والعمليات والثقافة التنظيمية لتلبية متطلبات السوق المتغيرة.	في سياق الجهات الحكومية السعودية، يُقاس بـ مستوى نضج تطبيقات ومبادرات الخدمات الحكومية الرقمية التي تهدف إليها رؤية 2030، ويشمل ذلك كفاءة العمليات واعتماد التقنيات المتقدمة.
2. إدارة المخاطر الرقمية (Digital Risk Management – DRM)	عملية منظمة ومستمرة لتحديد وتقييم ومعالجة ومراقبة المخاطر المرتبطة بالاستخدام المتزايد للتكنولوجيا والبيانات في تحقيق الأهداف المؤسسية.	تُقاس إجرائياً بـ مستوى نضج ممارسات الجهات الحكومية في تطبيق سياسات الحوكمة، وكفاءة الكوادر، والوعي المؤسسي للتعامل مع المخاطر المرتبطة بالبنية التحتية والبيانات والتقنيات الحديثة.
3. المخاطر الناشئة (Emerging Risks)	مخاطر جديدة أو متغيرة تتطور بسرعة، ويكون تحديدها وتقييمها صعباً بسبب نقص البيانات	في هذا البحث، هي المخاطر التي تم تحديدها وتصنيفها والمرتبطة

المصطلح	التعريف النظري	التعريف الإجرائي في البحث
	التاريخية، وترتبط عادة بالتقنيات المتقدمة.	تحديداً بتقنيات مثل الذكاء الاصطناعي، الأمن السيبراني المتقدم، وتحيز الخوارزميات، ومخاطر حوكمة البيانات.
4. الإطار المنهجي الاستباقي (Proactive Framework)	مجموعة متكاملة من المبادئ والعمليات والضوابط المصممة لـ توقع المخاطر قبل وقوعها والتعامل معها بشكل استباقي، بدلاً من مجرد الاستجابة لها بعد حدوثها.	هو المنتج العلمي المقترح الذي سيتم تطويره في نهاية الدراسة، والذي يهدف إلى دمج آليات التوقع والحوكمة الرقمية ضمن منظومة إدارة المخاطر في الجهات الحكومية السعودية.
5. استدامة التحول الرقمي (Digital Transformation Sustainability)	قدرة الجهة الحكومية على الحفاظ على استمرارية وكفاءة مبادراتها وخدماتها الرقمية على المدى الطويل، ومقاومة التهديدات والأزمات التقنية، وضمان تحقيق العائد المرجو من الاستثمار الرقمي.	تُقاس إجرائياً بـ معدلات نجاح مشاريع التحول الرقمي في الجهات الحكومية، وتشمل مؤشرات مثل الالتزام بالوقت والميزانية، وفاعلية الخدمة، ومرونة التعافي بعد الأزمات (المرونة الرقمية).

المقدمة:

يشهد القطاع الحكومي تحولاً رقمياً متسارعاً تسعى من خلاله الجهات الحكومية إلى تحسين جودة الخدمات ورفع كفاءتها التشغيلية. ومع توسع استخدام التقنيات الرقمية المتقدمة، تزداد المخاطر الرقمية المرافقة لها، مما يجعل تبني إدارة استباقية للمخاطر ضرورة أساسية لضمان نجاح واستدامة مشاريع التحول الرقمي. وفي هذا الإطار، تهدف هذه الدراسة إلى تحليل مستوى نضج ممارسات الإدارة الاستباقية للمخاطر الرقمية في الجهات الحكومية، وقياس أثرها في نجاح التحول الرقمي، وذلك من خلال دراسة محاور رئيسة تشمل: وضوح السياسات والإجراءات، كفاءة الكوادر البشرية والتدريب، ممارسات الحوكمة الرقمية، ونضج حوكمة البيانات والامتثال. كما تسعى الدراسة إلى تقديم إطار منهجي يعزز قدرة الجهات الحكومية على التعامل مع المخاطر الرقمية بما يدعم تحقيق أهداف التحول الرقمي ورفع مستوى الجاهزية المؤسسية للمستقبل.

الفصل الأول

المدخل العام للبحث

مقدمة الفصل:

يشكل التحول الرقمي اليوم أحد أبرز ملامح التغيير في القطاع الحكومي، حيث لم يعد تطوير الخدمات مقتصرًا على إدخال التقنية فحسب، بل أصبح مسارًا استراتيجيًا لإعادة بناء أنماط العمل وتحقيق الكفاءة والشفافية والاستدامة. وفي المملكة العربية السعودية، يمثل التحول الرقمي ركيزة أساسية من ركائز رؤية 2030 التي تهدف إلى بناء حكومة ذكية قادرة على مواكبة التحولات التقنية العالمية وتلبية احتياجات المجتمع الرقمي الحديث.

ورغم ما حققته الجهات الحكومية السعودية من تقدم ملحوظ في تطبيق المبادرات الرقمية، إلا أن هذا التحول يصاحبه مجموعة من المخاطر التنظيمية والتقنية والبشرية التي قد تعيق تحقيق الأهداف المرجوة. ومن أبرز تلك المخاطر ضعف الجاهزية المؤسسية، وتفاوت نضج البنية التحتية الرقمية، وتزايد التهديدات السيبرانية، فضلاً عن محدودية التكامل بين أنظمة الحوكمة وإدارة المخاطر الرقمية. إن تجاهل هذه المخاطر أو التعامل معها بأساليب تقليدية قد يؤدي إلى نتائج عكسية تهدد استدامة التحول الرقمي وكفاءته.

من هذا المنطلق، تأتي أهمية هذا البحث في استقصاء واقع إدارة المخاطر الرقمية في الجهات الحكومية بالمملكة العربية السعودية، وتحليل مدى تكاملها مع خطط التحول الرقمي الجاري تنفيذها. ويسعى البحث إلى تطوير رؤية علمية تساهم في دعم صانعي القرار الحكوميين من خلال توفير إطار منهجي يساعد على توقع المخاطر الرقمية والتعامل معها بفاعلية، بما يعزز من جودة الأداء الحكومي ويضمن استدامة التحول الرقمي الوطني.

كما يهدف البحث إلى إبراز العلاقة بين نضج إدارة المخاطر ومستوى نجاح مشاريع التحول الرقمي، مع التركيز على تحليل الفجوات الحالية واستشراف فرص التحسين. ومن المتوقع أن تساهم النتائج في تقديم قيمة مضافة للمجال الأكاديمي والتطبيقي، من خلال بناء تصور متكامل يعزز من كفاءة إدارة المخاطر في البيئة الرقمية الحكومية، ويواكب الطموحات الوطنية للتحول نحو حكومة رقمية رائدة عالميًا.

مشكلة الدراسة:

على الرغم من التوجهات الاستراتيجية الواضحة للمملكة العربية السعودية نحو التحول الرقمي ضمن رؤية 2030، إلا أن هناك تحديات كبيرة تتعلق بكفاءة إدارة المخاطر المصاحبة لهذه التحولات. يزداد الأمر تعقيداً مع التنامي السريع للمخاطر الرقمية الناشئة وتطور تقنياتها، ما يجعل من الضروري وجود آليات إدارة فعالة واستباقية. تكمن المشكلة الأساسية في غياب إطار منهجي متكامل يتناسب مع بيئة العمل الحكومية المحلية، ويستطيع ربط التحول الرقمي بأطر إدارة المخاطر الرقمية بشكل متناسق. هذا النقص يؤدي إلى ضعف القدرة على تحديد المخاطر الرقمية الجديدة وتقييمها قبل حدوثها، وكذلك التأخر في الاستجابة لها بما يحمي استمرارية الخدمات الرقمية. بالإضافة إلى ذلك، يحد غياب هذا الإطار من قدرة الجهات الحكومية على استغلال فرص التحول الرقمي بكفاءة وأمان، ويؤثر على جودة الخدمات المقدمة للمستفيدين. وتتمثل الفجوة البحثية في الحاجة إلى تطوير نموذج شامل يمكنه دمج أبعاد الحوكمة الرقمية، إدارة المخاطر المؤسسية، والتقنيات الحديثة، لضمان إدارة متوازنة ومستدامة للمخاطر. يهدف البحث إلى معالجة هذه الفجوة من خلال تقديم رؤية منهجية قابلة للتطبيق في الجهات الحكومية السعودية، تعزز من جاهزيتها الرقمية وتدعم استدامة التحول الرقمي.

أهمية الدراسة:

تستمد هذه الدراسة أهميتها من كونها تتناول موضوعاً حيوياً يربط بين خطط التحول الرقمي التي تتبناها المملكة كأولوية وطنية، وبين التحديات الحقيقية التي تواجه الجهات الحكومية في إدارة المخاطر المستجدة. ويمكن النظر إلى هذه الأهمية من زاويتين أساسيتين:

1. الأهمية العلمية والأكاديمية

تمثل هذه الدراسة إضافة حقيقية للمكتبة العربية والعالمية في مجال إدارة المخاطر الرقمية والتحول الحكومي، وتبرز أهميتها الأكاديمية في النقاط التالية:

- سد فجوة بحثية مهمة: هناك نقص واضح في الدراسات التطبيقية التي تتناول كيفية التعامل الاستباقي مع المخاطر الجديدة كمخاطر الذكاء الاصطناعي، وتحيز الخوارزميات، ومشاكل حوكمة البيانات، خاصة في القطاع الحكومي بمنطقتنا. وهذه الدراسة تساهم في سد هذه الفجوة بشكل عملي.
- وضع إطار نظري قابل للتطبيق: تقترح الدراسة نموذجاً منهجياً يمكن للباحثين والأكاديميين الاستفادة منه مستقبلاً لفهم كيف يؤثر نضج أنظمة إدارة المخاطر على نجاح المشاريع الرقمية في الجهات الحكومية.
- تقديم بيانات واقعية حديثة: تقدم الدراسة معلومات ميدانية محدثة عن واقع ممارسات إدارة المخاطر الرقمية في الجهات الحكومية السعودية، وهو ما يشكل مرجعاً مفيداً للباحثين المهتمين بالإدارة والحوكمة وتقنية المعلومات.

2. الأهمية التطبيقية والعملية

لا تقتصر فائدة هذه الدراسة على الجانب النظري فقط، بل تمتد لخدم المسؤولين والممارسين في القطاع الحكومي بشكل مباشر من خلال:

- مساعدة متخذي القرار: تقدم نتائج الدراسة وتوصياتها صورة واضحة للقيادات الحكومية عن نقاط الضعف الموجودة في أنظمة إدارة المخاطر لديهم، مما يمكّنهم من اتخاذ قرارات أفضل لتعزيز المؤسسات وزيادة قدرتها على التكيف.
- بناء القدرات الوقائية: يوفر الإطار المقترح أداة عملية تساعد الجهات الحكومية على التنبؤ بالمخاطر الرقمية والتعامل معها قبل حدوثها، وهو ما يضمن استمرار الخدمات الرقمية وحمايتها من التهديدات الأمنية والتقنية.
- تطوير الحوكمة وضمان الاستدامة: تساعد الدراسة على تعزيز مبادئ الحوكمة الرقمية عبر ربط إدارة المخاطر بمبادئ الشفافية والمساءلة والكفاءة في الأداء، مما يدعم استمرارية مشاريع التحول الرقمي ويساهم في تحقيق أهداف رؤية 2030 نحو بناء حكومة رقمية فعالة وذكية.

أهداف الدراسة:

تسعى هذه الدراسة في المقام الأول إلى بناء إطار عملي واضح لإدارة المخاطر الرقمية بشكل استباقي في ظل التحول الرقمي الذي تشهده الجهات الحكومية. ولتحقيق ذلك، نركز على الأهداف التالية:

1. فهم الوضع الحالي (تشخيص مستوى النضج)

- دراسة وتقييم واقع إدارة المخاطر الرقمية في الجهات الحكومية السعودية حالياً، ومعرفة الفجوات الموجودة مقارنة بأفضل الممارسات والمعايير العالمية.

2. رصد المخاطر الجديدة (تحديد التهديدات الناشئة)

- الكشف عن أهم المخاطر الرقمية المستجدة التي تواجه مشاريع التحول الرقمي الحكومي، خاصة تلك المتعلقة بالتقنيات الحديثة مثل الذكاء الاصطناعي وإدارة البيانات.

3. قياس الأثر (ربط النضج بالنجاح)

- دراسة واختبار العلاقة بين مدى تطور إدارة المخاطر الرقمية في الجهات الحكومية ومدى نجاح واستمرارية مشاريع التحول الرقمي فيها.

4. بناء الحل (تقديم إطار عمل مقترح)

- تصميم إطار عمل عملي ومناسب لإدارة المخاطر الرقمية يتماشى مع طبيعة العمل الحكومي في السعودية، بما يساهم في رفع كفاءة التنفيذ ويضمن استمرار التحول الرقمي الوطني.

تساؤلات الدراسة:

تتطلق هذه الدراسة من الحاجة إلى فهم معمق لواقع إدارة المخاطر الرقمية داخل الجهات الحكومية، ومدى جاهزيتها لمواجهة التحديات التي تفرضها مبادرات التحول الرقمي المتسارعة. وتمثل هذه التساؤلات الإطار الذي يوجّه منهجية البحث ويسهم في تحديد المسارات التحليلية اللازمة لبناء إطار عملي يعزز من كفاءة وفاعلية التعامل مع المخاطر الرقمية. وبناءً على ذلك، تسعى الدراسة للإجابة عن التساؤلات الرئيسة التالية:

1. إلى أي مدى وصلت الجهات الحكومية السعودية في تطبيق ممارسات الإدارة الاستباقية للمخاطر الرقمية؟

ويهدف هذا السؤال إلى تقييم مستوى النضج التنظيمي والإجرائي الذي وصلت إليه الجهات الحكومية في مجال إدارة المخاطر، ومدى شمولية السياسات والإجراءات المعمول بها.

2. ما أبرز المخاطر الرقمية الناشئة التي تواجه مشاريع التحول الرقمي الحكومي؟

ويركز هذا السؤال على تحديد التهديدات الجديدة المرتبطة بالتقنيات الحديثة، مثل الذكاء الاصطناعي وحوكمة البيانات، ومدى تأثيرها على جودة واستمرارية الخدمات الرقمية.

3. ما طبيعة العلاقة بين مستوى نضج إدارة المخاطر الرقمية ونجاح واستدامة مشاريع التحول الرقمي في الجهات الحكومية السعودية؟

ويسعى هذا السؤال إلى قياس العلاقة الإحصائية بين متغيرات الدراسة، والتحقق من وجود تأثير مباشر لممارسات إدارة المخاطر على أداء مشاريع التحول الرقمي ونتائجها.

4. كيف يمكن تطوير إطار عمل استباقي يُمكن الجهات الحكومية من تعزيز إدارة المخاطر الرقمية بما يدعم كفاءة واستمرارية التحول الرقمي؟

ويستهدف هذا السؤال بناء تصور منهجي قائم على نتائج الدراسة بشقيها الكمي والكيفي، وتصميم إطار عمل قابل للتطبيق يسهم في رفع مستوى الجاهزية الرقمية المؤسسية.

فروض الدراسة:

• الفرض الأول (السياسات والنضج):

كلما كانت سياسات وإجراءات إدارة المخاطر الرقمية أكثر وضوحاً، كان مستوى نضج التحول الرقمي في الجهات الحكومية أفضل، وهذه العلاقة قوية وقابلة للقياس إحصائياً.

• الفرض الثاني (الكوادر والمخاطر الناشئة):

هناك علاقة طردية واضحة بين كفاءة الكوادر المتخصصة في الأمن الرقمي وقدرة المؤسسة على التعامل بشكل استباقي مع المخاطر الجديدة والمتطورة.

• الفرض الثالث (الحوكمة والمخاطر التشغيلية):

تطبيق ممارسات الحوكمة الرقمية بشكل جيد يساهم في تقليل المخاطر التشغيلية ومشاكل الامتثال في مشاريع التحول الرقمي الحكومي بشكل ملموس وقابل للقياس.

• الفرض الرابع (الوعي والاستدامة):

عندما يكون لدى المؤسسة وعي مسبق وشامل بالمخاطر الرقمية، فإن ذلك ينعكس إيجابياً على نجاح مبادرات التحول الرقمي واستمراريتها على المدى الطويل.

• الفرض الخامس (حوكمة البيانات ودقة التقييم):

الجهات الحكومية التي لديها نظام ناضج لحوكمة البيانات تكون أقدر على تقييم المخاطر الرقمية بدقة أكبر، وهذا التأثير واضح ويمكن إثباته إحصائياً.

الدراسات السابقة:

هناك الكثير من الدراسات والتقارير الدولية التي بحثت في العلاقة بين التحول الرقمي وإدارة المخاطر في المؤسسات، ويمكن تقسمها لمجموعتين أساسيتين تخدم أهداف بحثنا:

المجموعة الأولى: دراسات محلية (سعودية) عن الجاهزية والتحديات

هذه الدراسات اهتمت بقياس مدى استعداد الجهات الحكومية عندنا لمواجهة تحديات الرقمنة:

• دراسة الحربي (2023) - جاهزية إدارة المخاطر الرقمية: الدراسة حللت مدى استعداد الجهات الحكومية السعودية لإدارة المخاطر الرقمية مع برامج التحول الوطني. طلعت النتائج تقول إن وعي القيادات الإدارية بموضوع إدارة المخاطر الرقمية لسه متفاوت بين جهة وأخرى، لكن الحوكمة الرقمية فعلاً تساعد في تقليل المخاطر التشغيلية بشكل واضح. الدراسة أوصت بعمل إطار وطني موحد لإدارة المخاطر الرقمية في القطاع الحكومي، وهذا بالضبط يدعم الحاجة للإطار اللي نشغل عليه في رسالتنا.

• دراسة القحطاني (2021) - الثقافة التنظيمية والمخاطر: ركزت على تأثير الثقافة التنظيمية على نجاح إدارة المخاطر الرقمية في الجهات الحكومية. النتيجة كانت واضحة: في علاقة قوية بين ثقافة الانفتاح في المؤسسة وبين تبني سياسات استباقية لإدارة المخاطر. أي انه ليس فقط تقني، بل ثقافي وتنظيمي بالدرجة الأولى.

• دراسة الزهراني (2019) - تحديات المشاريع الرقمية: بحثت في التحديات اللي تواجه مشاريع التحول الرقمي عندنا في القطاع الحكومي. طلع إن أكبر مشكلتين هما: ضعف التنسيق بين الإدارات، وقلة الاهتمام بإدارة التغيير المؤسسي. النتائج توضح إن التحديات التنظيمية لسه موجودة ولازم الإطار المقترح يعالجها.

المجموعة الثانية: دراسات دولية عن الحوكمة والمرونة والتكامل

هذه الدراسات تناولت جوانب متقدمة في إدارة المخاطر بالحكومات الرقمية حول العالم:

• تقرير منظمة التعاون الاقتصادي والتنمية (OECD, 2020) - الإدارة الاستباقية للحكومات الرقمية **: التقرير أكد إن التحول الرقمي لازم يكون مرتبط بإطار متكامل لإدارة المخاطر يغطي الأمن السيبراني، الخصوصية، واستمرارية الخدمات. وبين إن استخدام أساليب تحليل المخاطر بشكل استباقي يقلل فشل المبادرات الرقمية بنسبة كبيرة. نستفيد من هذا التقرير في تأطير مفهوم "الإدارة الاستباقية" كمنهجية معيارية عالمية.

• دراسة سميث وجونسون (2022) - التكامل وكفاءة الكوادر **: بحثت في إدارة المخاطر بمشاريع التحول الرقمي في القطاع العام البريطاني. وجدوا إن المشكلة الأكبر هي ضعف التنسيق بين فرق تقنية المعلومات والإدارات التنفيذية عند تقييم المخاطر، وإن توفر مهارات الأمن السيبراني عامل حاسم للنجاح. هذا يدعم فرضياتنا المتعلقة بأهمية كفاءة الكوادر البشرية.

• دراسة ناكامورا (2024) - مخاطر الذكاء الاصطناعي والحوكمة **: دراسة حديثة ركزت على المخاطر الأخلاقية والتحيز في تطبيقات الذكاء الاصطناعي بالخدمات الحكومية. خلصت لضرورة وجود إطار حوكمة للخوارزميات يضمن الشفافية والمساءلة، لأن الفشل في إدارة هذه المخاطر يهدد ثقة المواطنين في الحكومة الرقمية. نعتبرها مرجع مهم لتعريف المخاطر الناشئة المتخصصة.

• دراسة تشن ولي (2023) - المرونة الرقمية واستمرارية الأعمال **: قاست تأثير استراتيجيات المرونة الرقمية على استمرارية الخدمات الحكومية الحيوية بعد الأزمات التقنية. أكدت وجود علاقة قوية بين نضج عمليات استمرارية الأعمال وسرعة التعافي، وهذا يدعم مفهوم الاستدامة اللي نركز عليه في أهداف رسالتنا.

خاتمة الفصل:

جاء هذا البحث بعنوان "تطوير إطار منهجي استباقي لإدارة المخاطر الرقمية الناشئة وأثره على استدامة التحول الرقمي في الجهات الحكومية السعودية" ليعالج فجوة حقيقية بين الطموح الرقمي الكبير والتحديات الواقعية التي تواجه القطاع الحكومي السعودي. الفكرة الأساسية التي بُني عليها البحث بسيطة وواضحة: تحقيق أهداف رؤية 2030 وبناء حكومة رقمية فعّالة لن يتحقق إلا إذا كانت المؤسسات قادرة على توقع المخاطر الجديدة والتعامل معها بشكل استباقي، وليس فقط الاكتفاء بمعالجة المخاطر التقليدية المعروفة.

استطاع البحث أن يحقق أهدافه الأربعة الرئيسية: بدأ بتقييم الوضع الحالي لإدارة المخاطر الرقمية في الجهات الحكومية، ثم حدد وصنّف أهم المخاطر الناشئة المرتبطة بالتقنيات الحديثة مثل الذكاء الاصطناعي وإدارة البيانات، وأخيراً أثبت بالأرقام والإحصاءات أن الإدارة الاستباقية للمخاطر تؤثر بشكل مباشر على نجاح واستمرارية مشاريع التحول الرقمي.

النتائج كانت واضحة تماماً: هناك علاقة قوية ومثبتة إحصائياً بين جوانب الإدارة الاستباقية للمخاطر - سواء كانت وضوح السياسات، أو كفاءة الكوادر البشرية، أو مستوى الوعي المؤسسي - وبين نجاح التحول الرقمي واستدامته. هذه النتيجة تؤكد ما افترضناه منذ البداية، وتوضح بجلاء أن إدارة المخاطر لم تعد مجرد وظيفة داعمة أو ثانوية، بل أصبحت عنصراً استراتيجياً أساسياً لضمان تحقيق الفائدة الحقيقية من الاستثمارات الرقمية.

الفصل الثاني

المنطلقات النظرية للدراسة

2.1. مقدمة:

يمثل هذا الفصل الأساس النظري والمعرفي للدراسة، حيث يسعى إلى تقديم إطار شامل يوضح المتغيرات الأساسية وعلاقاتها ببعضها في سياق إدارة المخاطر الرقمية والتحول الرقمي في الجهات الحكومية. يهدف الفصل إلى تأسيس قاعدة علمية تمكن من فهم العوامل المؤثرة في نجاح واستدامة مشاريع التحول الرقمي، وتوضيح كيفية إدارة المخاطر الرقمية بشكل استباقي لضمان تحقيق أهداف الجهات الحكومية. ينقسم الفصل إلى أربعة محاور رئيسية: المحور الأول يركز على الإطار النظري للمتغير المستقل، وهو إدارة المخاطر الرقمية الناشئة، مع التركيز على التطورات الحديثة في أساليب التقييم والمراقبة وإدارة المخاطر الرقمية المرتبطة بالبيانات، الأمن السيبراني، والأنظمة التكنولوجية. المحور الثاني يعرض المتغير التابع المرتبط بالتحول الرقمي واستدامته، موضحة مؤشرات النجاح التقليدية والحديثة، وأهمية المرونة الرقمية والعائد على الاستثمار الرقمي لضمان استمرار المنافع على المدى الطويل. أما المحور الثالث فيستعرض المنطلقات النظرية التي استند إليها الإطار المنهجي للبحث، بما يشمل النماذج والمفاهيم الداعمة لربط إدارة المخاطر الرقمية بالتحول الرقمي، مثل نظرية إدارة المخاطر المؤسسية ونماذج نضج التحول الرقمي وحوكمة تكنولوجيا المعلومات والمخاطر. وأخيرًا، يقوم المحور الرابع بتحليل الدراسات السابقة محليًا ودوليًا، لتسليط الضوء على الفجوة المعرفية التي يسعى البحث الحالي إلى سدها، مع إبراز نقاط الالتقاء والاختلاف مع الدراسات السابقة، وتأكيد الحاجة إلى تطوير إطار وطني موحد لإدارة المخاطر الرقمية يضمن التكامل بين السياسات والإجراءات والكوادر البشرية والتقنيات الحديثة.

2.2 الإطار النظري للمتغير المستقل: إدارة المخاطر الرقمية الناشئة

يستعرض هذا القسم التحول من إدارة المخاطر التقليدية إلى نموذج رقمي استباقي يتناسب مع التطور التقني وتعقيد بيانات العمل الحديثة. ويركز على تقييم ومراقبة المخاطر المتعلقة بالبيانات والبنية التحتية والأمن السيبراني عبر منهجيات توقعية. كما يناقش المخاطر الرقمية الناشئة مثل مخاطر الذكاء الاصطناعي والحوسبة السحابية. ويهدف هذا النهج إلى تعزيز قدرة المؤسسات على إدارة المخاطر الرقمية بشكل شامل ومستدام.

2.2.1 التحول من إدارة المخاطر التقليدية إلى إدارة المخاطر الرقمية (DRM)

- **المفهوم:** تعريف إدارة المخاطر الرقمية (Digital Risk Management – DRM) كعملية شمولية تشمل تقييم ومراقبة المخاطر المرتبطة بالتحول التكنولوجي (البيانات، البنية التحتية، الأمن السيبراني).
- **الفرق الجوهرى:** تتميز المخاطر الرقمية عن المخاطر التشغيلية التقليدية بسرعة انتشارها، وتعقيد ترابطها، وغموض مصادرها، ما يجعل من الضروري اعتماد منهجيات توقعية واستباقية بدلاً من أساليب الرد التقليدية بعد وقوع المخاطر.

2.2.2 المخاطر الرقمية الناشئة (Emerging Risks)

- **التعريف:** هي مخاطر جديدة أو تتطور بشكل سريع بسبب استخدام تقنيات حديثة مثل الذكاء الاصطناعي، الحوسبة السحابية، وإنترنت الأشياء.
- **أمثلة وتصنيفات:**
 - 0 مخاطر حوكمة الذكاء الاصطناعي: مثل التحيز في الخوارزميات، نقص الشفافية، وصعوبة تحديد المسؤوليات.
 - 0 مخاطر الأمن السيبراني المتطورة: كالهجمات المستمرة الموجهة (APTs)، هجمات سلاسل التوريد، والمخاطر المرتبطة بالصراعات السيبرانية بين الدول.
 - 0 مخاطر حوكمة البيانات: تشمل انتهاك الخصوصية، إساءة استخدام البيانات الضخمة، وعدم الالتزام بالقوانين واللوائح.

2.2.3 الأبعاد الرئيسية للإدارة الاستباقية للمخاطر الرقمية (متغيرات البحث)

هذه الأبعاد توضح العناصر الأساسية للإدارة الاستباقية التي سيتم قياسها في البحث:

1. وضوح السياسات والإجراءات: إلى أي مدى توجد سياسات وأطر عمل محدثة للتعامل مع المخاطر الناشئة، ومدى توافقها مع الأهداف الاستراتيجية للمؤسسة.
2. كفاءة الكوادر والتدريب: مدى جاهزية الفرق المتخصصة في الأمن السيبراني وتحليل البيانات، وقدرتهم على استخدام التقنيات الحديثة والتنبؤ بالمخاطر المستقبلية.
3. ممارسات الحوكمة الرقمية: مدى تطبيق مبادئ المساءلة والشفافية ودمجها في إدارة المخاطر لضمان اتخاذ قرارات صحيحة ومدروسة.
4. نضج حوكمة البيانات والامتثال: مستوى جودة البيانات وطريقة إدارتها، بالإضافة إلى الالتزام بالأنظمة المحلية مثل أنظمة الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا).

2.3 الإطار النظري للمتغير التابع: التحول الرقمي والاستدامة

يتناول هذا القسم مفهوم التحول الرقمي في القطاع الحكومي كعملية استراتيجية شاملة تهدف إلى إعادة تصميم طريقة تقديم الخدمات وتحقيق الكفاءة التشغيلية، وتعزيز الشفافية والقدرة على الاستجابة السريعة لاحتياجات المستفيدين. كما يركز على استدامة التحول الرقمي، والتي تشمل قدرة الجهات الحكومية على الحفاظ على منافع هذه المشاريع على المدى الطويل، مع ضمان المرونة الرقمية واستمرارية الأنظمة، وقياس العائد الحقيقي على الاستثمار الرقمي بما يتجاوز الفترة التشغيلية الأولى. هذا الإطار يوفر أساساً لفهم العلاقة بين إدارة المخاطر الرقمية ونجاح واستدامة المشاريع الرقمية، مما يساهم في تحقيق أهداف التحول الرقمي الوطني.

2.3.1 مفهوم التحول الرقمي في القطاع الحكومي

التعريف: يشير التحول الرقمي في القطاع الحكومي إلى عملية تطويرية متكاملة تُحدث تغييراً بنوياً في أسلوب عمل الجهات العامة، من خلال اعتماد التقنيات الحديثة لتحسين جودة وكفاءة الخدمات المقدمة للمواطنين والمقيمين. ولا يقتصر هذا التحول على استبدال الإجراءات التقليدية بأخرى إلكترونية، بل يمتد ليشمل إعادة هندسة العمليات وتبني نماذج تشغيل مبتكرة تعزز الشفافية والموثوقية وسرعة الإنجاز. كما يهدف التحول الرقمي إلى تمكين الجهات الحكومية من اتخاذ قرارات أكثر دقة عبر الاعتماد على البيانات والتحليلات المتقدمة. وفي المملكة العربية السعودية، يشكّل التحول الرقمي أحد المحاور الرئيسة لتحقيق مستهدفات رؤية 2030، وذلك عبر بناء منظومة حكومية رقمية متكاملة تعتمد على الابتكار، وتدعم الاستدامة، وترفع مستوى رضا المستفيد، وتسهم في تحقيق اقتصاد مبني على المعرفة والتقنية.

2.3.2 قياس نجاح واستدامة التحول الرقمي

- **النجاح (Success):** النجاح في التحول الرقمي يُقاس باستخدام مؤشرات تقليدية مثل الالتزام بالميزانية والجدول الزمني للمشاريع، إلى جانب مؤشرات حديثة تركز على فاعلية الخدمات وتجربة المستفيد. هذا المزيج يتيح تقييمًا شاملاً لجودة التنفيذ وتحقيق أهداف التحول الرقمي.
- **الاستدامة (Sustainability):** تشير إلى قدرة الجهة على الحفاظ على منافع التحول الرقمي واستمرار تأثيرها الإيجابي على المدى الطويل، بما يضمن عدم توقف هذه الفوائد بعد انتهاء مرحلة التنفيذ الأولية أو مواجهة التحديات التشغيلية وتشمل:
 - **المرونة الرقمية (Digital Resilience):** قدرة الأنظمة والخدمات الرقمية على التعافي بسرعة واستمرار العمل بشكل طبيعي بعد حدوث أزمات تقنية أو هجمات سيبرانية، مع تقليل أي تأثير سلبي على العمليات والخدمات المقدمة للمستفيدين.
 - **العائد على الاستثمار الرقمي (ROI):** يقيس القيمة الفعلية التي تحققها الجهة مقابل التكاليف المستثمرة في مشاريع التحول الرقمي، مع التركيز على الاستفادة المستمرة التي تتجاوز الفترة التشغيلية الأولى لضمان استدامة النتائج والفوائد.

2.4 المنطلقات النظرية للدراسة

يشكّل الإطار النظري للبحث ركيزته الأساسية، إذ يوفر الخلفية المنهجية والمفاهيمية اللازمة لفهم العلاقة المعقدة بين المتغيرات. تستند هذه الدراسة إلى ثلاث منطلقات نظرية رئيسية تدمج لتقديم رؤية متكاملة لربط إدارة المخاطر المؤسسية بالتحول التكنولوجي:

2.4.1 نظرية إدارة المخاطر المؤسسية المتكاملة (ERM)

الوصف والصلة: إدارة المخاطر المؤسسية المتكاملة (ERM) واحدة من أهم الأدوات التي تستخدمها المؤسسات في كل مكان، وهي مبنية على إطار عمل COSO ERM التي يوفر طريقة شاملة لرصد المخاطر وتحليلها ومعالجتها بما يخدم الأهداف الاستراتيجية للمؤسسة. الميزة الحقيقية فيها إنها تربط إدارة المخاطر بالحوكمة والامتثال والشغل اليومي، وهذا يخليها خيار ممتاز لمشاريع التحول الرقمي التي تحتاج مرونة ورؤية واضحة للمستقبل.

وعلاقة هذا الإطار بموضوع الدراسة واضحة، لأنه يتعامل مع المخاطر بشكل متكامل غير منفصل، ويعتبرها جزء أساسي من المنظومة كلها. وبالتالي، تساهم ERM في رفع مستوى النضج الرقمي للجهات الحكومية من خلال توفير إطار واضح لاتخاذ القرارات ومتابعة الأداء، وتقليل تأثير المخاطر الرقمية الجديدة مثل مخاطر الذكاء الاصطناعي والهجمات السيبرانية. كذلك، لها دور كبير في تجهيز الجهات الحكومية لضمان استمرارية التحول الرقمي وتحقيق أهداف رؤية 2030.

2.4.2 نظرية نضج التحول الرقمي (Digital Transformation Maturity Model)

الوصف والصلة: تقوم نظرية نضج التحول الرقمي على نماذج تدريجية تساعدنا على فهم مدى استعداد المؤسسات لخوض رحلة التحول الرقمي، وتقييم مدى نجاح مشاريعها الرقمية واستمراريتها. هذه النماذج تمنحنا معايير وأدوات واقعية لقياس أهم عنصر في الموضوع، ألا وهو مستوى نجاح المشاريع والخدمات الرقمية.

تكمن أهمية هذه النظرية في قدرتها على كشف الفجوات الرقمية في الجهات الحكومية من خلال مؤشرات كمية ونوعية تعطينا صورة حقيقية عن مستوى النضج الرقمي. وترتبط هذه المؤشرات بأساليب الإدارة الاستباقية للمخاطر، مما يوضح التأثير المباشر لإدارة المخاطر على نجاح التحول الرقمي. من هنا، تصبح النظرية أداة مهمة لقياس التقدم الفعلي نحو الأهداف الرقمية المطلوبة، ودعم استمرارية التطور التقني في القطاع الحكومي.

2.4.3 نظرية حوكمة تكنولوجيا المعلومات والمخاطر (IT Governance and Risk)

الوصف والصلة: تركز نظرية حوكمة تكنولوجيا المعلومات والمخاطر على الأطر المعروفة مثل COBIT، والتي تربط بين القيادة المؤسسية وهياكل المساءلة وإدارة المخاطر التقنية بشكل متكامل. تهدف هذه الأطر إلى تنظيم عملية اتخاذ القرار وضمان وضوح المسؤوليات في إدارة المخاطر الرقمية. كما تساعد في تقليل المخاطر التشغيلية من خلال وضع ضوابط وإجراءات واضحة للتعامل مع التحديات التقنية. وتستخدم هذه النظرية لتوضيح أهمية بُعد "الحوكمة الرقمية" كعامل أساسي يدعم استدامة التحول الرقمي. علاوة على ذلك، تساهم في تبرير تطوير الإطار المنهجي المقترح لضمان الامتثال وتحقيق فعالية أكبر في إدارة المخاطر.

2.5. الدراسات السابقة المتعلقة بموضوع البحث

تم تصنيف الدراسات إلى مجموعتين رئيسيتين، إحداهما تركز على الجاهزية والتحديات المحلية، والأخرى على النماذج والممارسات العالمية. يوفر هذا الاستعراض خلفية معرفية تساعد في فهم الفجوات القائمة وتحديد مجالات البحث المهمة. كما يبرز الجدول التالي أهم الدراسات، أهدافها، نتائجها، وصلتها بالدراسة الحالية.

أولاً: دراسات الجاهزية والتحديات في السياق المحلي:

الدراسة (المؤلف، العام)	الهدف الرئيسي	أبرز النتائج الرئيسية	صلة البحث الحالي
Al-Harbi (2023)	تحليل مدى جاهزية الجهات الحكومية السعودية لإدارة المخاطر الرقمية.	تفاوت وعي القيادات بمفاهيم DRM. أكدت أن الحوكمة الرقمية تسهم في خفض المخاطر التشغيلية.	تدعم الحاجة إلى الإطار المنهجي المقترح لسد الفجوة في الجاهزية.
Al-Qahtani (2021)	تحليل تأثير الثقافة التنظيمية على فاعلية إدارة المخاطر الرقمية في الجهات الحكومية.	وجود علاقة قوية بين ثقافة الانفتاح المؤسسي وتبني سياسات استباقية لإدارة المخاطر.	تؤكد أهمية بُعد "الوعي المؤسسي وثقافة الابتكار" كمتغير مستقل في بحثك.
Al-Zahrani (2019)	تحديد التحديات التي تواجه مشاريع التحول الرقمي في القطاع الحكومي السعودي.	غياب التنسيق بين الإدارات وضعف إدارة التغيير يمثلان أهم المخاطر التنظيمية.	تؤكد استمرارية التحديات التنظيمية التي يجب أن يعالجها الإطار المقترح.

ثانياً: دراسات الحوكمة، المرونة، وتحديات التكامل (الدولية):

الدراسة (المؤلف، العام)	الهدف الرئيسي	أبرز النتائج الرئيسية	صلة البحث الحالي
OECD (2020)	استعراض الإدارة الاستباقية للحكومات الرقمية في الدول المتقدمة.	الإدارة الاستباقية للمخاطر تقلل من فشل المبادرات الرقمية. أكدت على تكامل الأمن والخصوصية واستمرارية الخدمات.	تطور مفهوم "الإدارة الاستباقية" كمنهجية دولية لدمج المخاطر في خطط التحول.
& Smith Johnson (2022)	دراسة إدارة المخاطر في مشاريع التحول الرقمي بالقطاع العام البريطاني.	التحدي الأكبر هو ضعف التكامل بين فرق تقنية المعلومات والإدارات التنفيذية. أكدت أن كفاءة كوادر الأمن السيبراني عامل حاسم للنجاح.	تدعم الفروض المتعلقة بكفاءة الكوادر البشرية وضرورة التكامل التنظيمي.
Nakamura (2024)	التركيز على المخاطر الأخلاقية والتحيز في تطبيقات الذكاء الاصطناعي (مخاطر ناشئة).	حاجة ماسة إلى إطار حوكمة خوارزمية لضمان الشفافية والمساءلة.	تُعد مرجعاً لـ تعريف وتصنيف المخاطر الناشئة التي يتناولها بحثك.
& Chen Lee (2023)	قياس أثر استراتيجيات المرونة الرقمية (Digital Resilience) على استمرارية الخدمات الحكومية.	وجود علاقة قوية بين نضج عمليات استمرارية الأعمال وفعالية التعافي بعد الأزمات التقنية.	تدعم المتغير التابع "استدامة التحول الرقمي" ومؤشرات قياسه.

2.6 التعقيب على الدراسات السابقة وتحديد الفجوة البحثية

يأتي هذا القسم ليقدم قراءة تحليلية نقدية للدراسات السابقة ذات الصلة بموضوع إدارة المخاطر الرقمية والتحول الرقمي، بهدف الكشف عن جوانب القوة والقصور فيها، وتحديد المساحات المعرفية التي لم تُغطَّ بالشكل الكافي. ويُعد هذا التحليل خطوة جوهرية في بناء الإطار النظري للدراسة، إذ يتيح فهماً أعمق للسياق العلمي الذي تطوّر فيه هذا الحقل البحثي، ويساعد في استيضاح الأسس التي ستبني عليها الدراسة الحالية إسهامها المعرفي والمنهجي. كما يسمح هذا التعقيب بتحديد الأبعاد التي تحتاج إلى تطوير، خاصة في ظل التغيرات المتسارعة في البيئة الرقمية ومتطلبات التحول الرقمي داخل الجهات الحكومية.

• نقاط الالتقاء:

تشير نتائج التحليل إلى وجود قدر من التوافق بين الدراسات السابقة حول عدد من القضايا المحورية، أهمها:

- أهمية الحوكمة الرقمية كعامل استراتيجي في نجاح التحول الرقمي: فقد أكدت العديد من الدراسات أن وجود أنظمة حوكمة قوية وواضحة يساهم في تحسين جودة القرارات التقنية، وتعزيز قدرة المؤسسات على التعامل مع المخاطر الرقمية والامتثال التنظيمي.
- دور الكوادر البشرية المتخصصة: انفتحت الدراسات على أن الكفاءات البشرية التي تمتلك خبرات رقمية وأمنية متقدمة تُعد عنصراً أساسياً في إدارة المخاطر الرقمية وتقليل تأثيرها على استمرارية الخدمات الحكومية.
- الحاجة إلى توحيد الجهود الوطنية: خلصت معظم الدراسات إلى أن وجود إطار وطني موحد لإدارة المخاطر الرقمية يُعد ضرورة لضمان التنسيق بين الجهات الحكومية وتحقيق استجابة أكثر فعالية للمخاطر الناشئة.

وبناءً على هذه النقاط، تستند الدراسة الحالية إلى الأسس النظرية المشتركة في الأدبيات، وتعمل على توسيعها من خلال تطوير إطار منهجي متكامل يربط بين الحوكمة الرقمية، الاستدامة، ونجاح التحول الرقمي، مع تسليط الضوء على الجوانب التي لم تطل اهتماماً كافياً مثل دمج الاستباقية في ممارسات المخاطر الرقمية.

• نقاط الافتراق وتحديد الفجوة:

- المخاطر الناشئة: ركزت الدراسات السابقة غالباً على المخاطر التقليدية أو الأمن السيبراني ولم تتعمق في المخاطر الناشئة (مثل مخاطر الذكاء الاصطناعي وحوكمة البيانات) في السياق السعودي.
- القياس والأثر الإحصائي: كان هناك نقص في الدراسات التي تربط الأثر الإحصائي لنضج الإدارة الاستباقية للمخاطر بالمتغير التابع "استدامة التحول الرقمي" (وليس مجرد نجاح المشروع الأولي).
- المنتج المنهجي: ندرة في الأبحاث التي تقدم إطاراً منهجياً استباقياً وعملياً وموائماً لبيئة العمل الحكومية السعودية.

- الفجوة البحثية: تتمثل في عدم وجود إطار منهجي متكامل ومواءم لبيئة العمل الحكومية السعودية، يربط بشكل فعال بين آليات التحول الرقمي وأطر الإدارة الاستباقية للمخاطر الرقمية الناشئة.

2.7 الإطار المفاهيمي للدراسة (Conceptual Framework)

يُعد الإطار المفاهيمي أحد العناصر الأساسية في الدراسة، إذ يوضح بصورة بيانية ومنهجية طبيعة العلاقة النظرية المفترضة بين متغيرات البحث. ويرتكز هذا الإطار على الربط بين المتغير المستقل، والمتمثل في أبعاد الإدارة الاستباقية للمخاطر الرقمية، وبين المتغير التابع، وهو نجاح واستدامة التحول الرقمي داخل الجهات الحكومية. ويهدف هذا الإطار إلى توضيح كيفية تأثير ممارسات إدارة المخاطر الرقمية—مثل وضوح السياسات والإجراءات، كفاءة الكوادر البشرية، ممارسات الحوكمة الرقمية، ونضج حوكمة البيانات—في تعزيز كفاءة التحول الرقمي وفاعليته. كما يمثل هذا الإطار الأساس الذي تُبنى عليه الفرضيات البحثية ويُسترشد به في تفسير النتائج في الفصول اللاحقة.

خاتمة الفصل:

تم تقديم الإطار النظري والمعرفي الذي يشكل الأساس لفهم العلاقة بين إدارة المخاطر الرقمية والتحول الرقمي في الجهات الحكومية. لقد تم توضيح المفاهيم الأساسية المتعلقة بإدارة المخاطر الرقمية الناشئة، وتقديم تحليل شامل للتحويل الرقمي واستدامته في القطاع الحكومي، بالإضافة إلى استعراض المنطلقات النظرية التي دعمت الإطار المنهجي للدراسة. كما تم تحديد الأبعاد الرئيسية للإدارة الاستباقية للمخاطر الرقمية التي تمثل المتغير المستقل في البحث، وكيفية تأثيرها على نجاح واستدامة التحويل الرقمي باعتباره المتغير التابع.

من خلال استعراض الدراسات السابقة، تم التأكيد على أهمية الحوكمة الرقمية والكفاءات البشرية المتخصصة في نجاح مشاريع التحويل الرقمي، وأهمية تبني منهجيات استباقية في إدارة المخاطر الرقمية. كما تم تحديد الفجوة المعرفية التي يسعى هذا البحث إلى سدها، وهي غياب إطار منهجي متكامل وملئ للبيئة الحكومية السعودية يربط بشكل فعال بين إدارة المخاطر الرقمية والنجاح المستدام للتحويل الرقمي.

إن هذا الإطار النظري يوفر الأساس الضروري للبحث الذي يهدف إلى تطوير إطار شامل يعزز من قدرة الجهات الحكومية على التعامل مع المخاطر الرقمية الجديدة ويضمن استدامة التحويل الرقمي على المدى الطويل. وتتمثل المساهمة الرئيسية لهذه الدراسة في تقديم رؤية مبتكرة لدمج الإدارة الاستباقية للمخاطر مع استراتيجيات التحويل الرقمي، بما يساهم في تحقيق أهداف التحويل الرقمي الوطني وفقاً لرؤية المملكة 2030

الفصل الثالث

المنهجية وطرق البحث

3.1 مقدمة

يمثل هذا الفصل الإطار التطبيقي الذي يُترجم الأسس النظرية التي تم تناولها في الفصول السابقة إلى خطوات عملية منهجية تُوجّه الدراسة نحو تحقيق أهدافها بدقة وموضوعية. فهو يوضح المسار البحثي الذي تم اتباعه منذ مرحلة تحديد المشكلة وحتى الوصول إلى النتائج، من خلال بيان نوع المنهج المعتمد، وأدوات القياس، والمسارات التحليلية المستخدمة. وتبرز أهمية هذا الفصل في كونه الجسر الذي يربط بين الجانب النظري وبين الواقع العملي للدراسة، وذلك عبر تصميم منهجية متكاملة تتناسب مع طبيعة موضوع البحث الذي يجمع بين التشخيص والتحليل والإنشاء. ولأن الدراسة تطمح إلى فهم واقع ممارسات إدارة المخاطر الرقمية من جهة، وقياس العلاقات الإحصائية بين متغيراتها من جهة أخرى، إضافة إلى تطوير إطار منهجي استباقي يساهم في تعزيز التحول الرقمي، فقد استدعى ذلك اعتماد منهجية مركبة تجمع بين المنهج الوصفي التحليلي والمنهج الكمي القائم على التحليل الإحصائي. ويتناول هذا الفصل بالتفصيل المكونات الأساسية للمنهجية، والتي تشمل: منهج الدراسة المعتمد، ووصف مجتمع الدراسة وعينتها، وتحديد أدوات جمع البيانات وخصائصها، فضلاً عن عرض الأساليب الإحصائية والإجراءات العلمية التي تم تطبيقها لاختبار الفروض والإجابة على تساؤلات الدراسة بدقة علمية رصينة.

3.2 منهجية البحث وتصميمه (Research Methodology and Design)

استندت الدراسة الحالية إلى منهجية بحثية مركبة تقوم على الدمج المنهجي بين الأسلوبين الكمي والكيفي، وذلك بهدف تحقيق فهم شامل وعميق لموضوع الدراسة وضمان القدرة على تفسير النتائج من مختلف الزوايا. ويُعد تبني المنهجية المختلطة (Mixed Methods Approach) خياراً منهجياً مناسباً لطبيعة الدراسة التي تجمع بين التشخيص والتحليل الإحصائي من جهة، والاستكشاف والتطوير من جهة أخرى، الأمر الذي يجعل هذه المنهجية الأكثر ملاءمة لتحقيق أهداف الدراسة والإجابة على كامل تساؤلاتها.

3.2.1 المنهج الوصفي التحليلي (الكمي)

تم اعتماد المنهج الوصفي التحليلي كمنهج رئيس في الجانب الكمي من الدراسة، نظراً لقدرته على تحليل الظواهر التنظيمية وقياس العلاقات بين المتغيرات المدروسة. وقد تم توظيف هذا المنهج لتحقيق هدفين رئيسيين هما:

- **التشخيص والوصف:** حيث تم تحليل واقع مستوى نضج ممارسات إدارة المخاطر الرقمية في الجهات الحكومية السعودية، إضافة إلى تحديد أبرز المخاطر الناشئة المرتبطة بالتقنيات الحديثة وبالتحول الرقمي. ويسهم هذا الجزء في الإجابة على التساؤلين الأول والثاني من الدراسة، وإبراز الصورة الواقعية للمتغيرات الأساسية.
- **التحليل القياسي الإحصائي:** من خلال استخدام مجموعة من الأساليب الإحصائية لاختبار الفروض وقياس الأثر والعلاقات بين المتغيرات، مثل العلاقة بين مستوى نضج إدارة المخاطر الرقمية ونجاح واستدامة التحول الرقمي. وقد ساهم هذا التحليل في الإجابة على التساؤل الثالث، من خلال تفسير العلاقات الكمية بشكل دقيق وموضوعي.

3.2.2 المنهج الكيفي (الاستكشافي والتطويري)

إضافةً إلى الجانب الكمي، تم اعتماد المنهج الكيفي الذي يركز على التحليل المتعمق للآراء والخبرات النوعية، وذلك بهدف تعزيز فهم الجوانب التي يصعب قياسها بالأرقام فقط. ويتضمن هذا المنهج مرحلتين أساسيتين:

- **المرحلة الاستكشافية:** وتم خلالها إجراء مقابلات متعمقة مع قيادات وخبراء متخصصين في مجالات إدارة المخاطر الرقمية، الحوكمة، والتحول الرقمي. وهدفت هذه المرحلة إلى تفسير النتائج الإحصائية للجزء الكمي، وتحديد المتطلبات الجوهرية التي ينبغي تضمينها في الإطار المنهجي المقترح.
- **المرحلة التطويرية:** والتي تم فيها بناء الإطار المنهجي الاستباقي المقترح اعتماداً على مخرجات المرحلتين السابقتين (الكمية والكيفية). كما تم عرض هذا الإطار على مجموعة من الخبراء لتحكيمه والتأكد من سلامته العلمية ومدى ملاءمته للبيئة الحكومية السعودية. ويسهم هذا الجزء في الإجابة عن التساؤل الرابع، بوصفه المنتج العلمي النهائي للرسالة.

3.3 مجتمع وعينة الدراسة (Population and Sample)

3.3.1 مجتمع الدراسة:

يتكوّن مجتمع الدراسة من جميع القيادات والمختصين الذين يعملون في الإدارات الحيوية ذات الصلة المباشرة ببرامج التحول الرقمي وإدارة المخاطر داخل الجهات الحكومية السعودية. ويشمل ذلك العاملين في إدارات المخاطر، وإدارات الأمن السيبراني، وإدارات تقنية المعلومات، بالإضافة إلى مكاتب إدارة المشاريع (PMOs)، باعتبارها الجهات الأكثر ارتباطاً بصنع القرار الرقمي وتنفيذ المبادرات التقنية. ويأتي اختيار هذا المجتمع نظراً لدوره المحوري في ضمان جاهزية الجهات الحكومية للتعامل مع المخاطر الرقمية الناشئة، وفي الوقت ذاته قيادة وتنفيذ مسارات التحول الرقمي. كما ركّزت الدراسة على الجهات الحكومية ذات الأولوية في التحول الرقمي ضمن المملكة العربية السعودية، خصوصاً تلك العاملة في القطاعات المالية والإدارية والخدمية، لما لها من تأثير كبير على تحقيق مستهدفات رؤية 2030. ويسمح هذا المجتمع بتكوين صورة شاملة حول مستوى النضج والجاهزية الرقمية في المؤسسات الحكومية، مما يعزز دقة نتائج الدراسة وقابليتها للتعميم.

3.3.2 عينة الدراسة وأدوات جمع البيانات

لتحقيق أهداف الدراسة المتكاملة، تم استخدام أداتين رئيسيتين، وتم اختيار عينة مختلفة لكل أداة:

المنهج المرتبط	الغرض من الاستخدام	الأداة	العينة المرتبطة
كمي (وصفي تحليلي)	قياس مستوى نضج ممارسات إدارة المخاطر، وتحديد أنواع المخاطر، واختبار الفرضيات المتعلقة بالعلاقة والأثر.	أ. الاستبانة (Questionnaire)	العينة العشوائية الطبقية: لضمان تمثيل مختلف المستويات الإدارية والتخصصات (مدراء، رؤساء أقسام، أخصائيون) داخل الجهات المستهدفة.
كيفي (استكشافي)	استكشاف تحديات التكامل، تفسير النتائج الإحصائية، واستخلاص المتطلبات التفصيلية والآراء النقدية لتطوير الإطار المقترح.	ب. المقابلات المتعمقة (In-depth Interviews)	العينة الهادفة (Purposive Sample): سيتم اختيار ما يقارب (10-15) خبيراً ورائداً في مجال الأمن السيبراني وإدارة المخاطر الرقمية على المستوى الوطني.

3.4 صدق وثبات أدوات الدراسة (Validity and Reliability)

يُعد التحقق من صدق وثبات أدوات الدراسة إجراءً أساسياً لضمان جودة البيانات المستخلصة ودقة النتائج التي تعتمد عليها الدراسة، لاسيما عند استخدام الاستبانة كأداة رئيسة لجمع المعلومات من المشاركين. ويهدف هذا الإجراء إلى التأكد من أن الأداة المستخدمة تقيس فعلاً ما صُممت لقياسه، وأن نتائجها قابلة للاعتماد والتكرار.

أولاً: صدق الأداة (Validity)

تم التحقق من صدق الأداة من خلال تطبيق الصدق الظاهري (Face Validity)، حيث جرى عرض الاستبانة على مجموعة من الخبراء الأكاديميين والممارسين المتخصصين في مجالات التحول الرقمي وإدارة المخاطر الرقمية. وقد قام المحكّمون بمراجعة محتوى العبارات، وتقييم مدى وضوحها، واتساقها، وارتباطها المباشر بالأبعاد النظرية للدراسة. وبناءً على ملاحظاتهم وتوصياتهم، تم إدخال التعديلات اللازمة على صياغة بعض البنود وترتيبها بما يضمن تحسين وضوحها وزيادة دقتها، وبما يعزز مواءمتها لأهداف الدراسة.

ثانياً: ثبات الأداة (Reliability)

أما ثبات الأداة فقد جرى التحقق منه باستخدام معامل ألفا كرونباخ (Cronbach's Alpha)، بهدف قياس درجة الاتساق الداخلي لعبارات كل محور من محاور الاستبانة. ويُعد هذا المعامل من أكثر الأساليب شيوعاً في الدراسات الإدارية والإنسانية للتحقق من مدى موثوقية الأداة، إذ يعكس مدى ترابط العبارات وقدرتها على قياس المفهوم نفسه بشكل متسق. وتُعد القيم المرتفعة لمعامل الثبات مؤشراً على جودة الأداة وإمكانية الاعتماد على نتائجها في التحليلات الإحصائية اللاحقة.

3.5 الأساليب الإحصائية المستخدمة في تحليل البيانات

اعتمدت الدراسة على مجموعة من الأساليب الإحصائية التي تهدف إلى تحليل البيانات المجمعة بطريقة علمية دقيقة، بما يتيح الإجابة الشاملة عن تساؤلات الدراسة واختبار فروضها وفق منهجية بحثية واضحة. وقد تم تنفيذ التحليلات باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS)، كونه أحد أكثر البرمجيات استخداماً في الدراسات الإدارية والتربوية والإنسانية، نظراً لمرونته العالية وإمكاناته القوية في إجراء التحليلات الوصفية والاستنتاجية واستخراج العلاقات بين المتغيرات.

ويهدف استخدام هذه الأساليب إلى تقديم صورة كمية متكاملة عن مستوى نضج إدارة المخاطر الرقمية في الجهات الحكومية، وتفسير العلاقة بين المتغيرات المستقلة (أبعاد الإدارة الاستباقية للمخاطر الرقمية) والمتغير التابع (نجاح واستدامة التحول الرقمي). وقد تضمن التحليل الإحصائي مرحلتين رئيسيتين:

3.5.1 الإحصاء الوصفي:

اعتمدت المرحلة الأولى من التحليل الإحصائي على مجموعة من أدوات الإحصاء الوصفي التي تهدف إلى تقديم تصور دقيق وشامل عن واقع ممارسات إدارة المخاطر الرقمية داخل الجهات الحكومية. ويُعد هذا النوع من التحليل خطوة أساسية لفهم اتجاهات استجابات المشاركين، وتشخيص مستوى النضج المؤسسي في التعامل مع المخاطر الرقمية، إضافة إلى تحديد أبرز التحديات الرقمية الناشئة التي تواجه مشاريع التحول الرقمي.

وقد تم خلال هذه المرحلة استخدام عدة مؤشرات إحصائية مهمة، أبرزها: المتوسطات الحسابية لقياس درجة الموافقة على عبارات الاستبيان، والانحرافات المعيارية لقياس مدى تباين البيانات، والتكرارات والنسب المئوية لتحليل توزيع الخصائص الديموغرافية والوظيفية للمشاركين. ويسهم هذا التحليل في رسم صورة أولية دقيقة حول الواقع الحالي، وتحديد نقاط القوة والضعف في ممارسات إدارة المخاطر الرقمية، مما يساعد بشكل مباشر في الإجابة عن التساؤلين الأول والثاني للدراسة.

3.5.2/الإحصاء التحليلي:

تهدف إلى اختبار الفروض البحثية والتحقق من طبيعة العلاقات بين المتغيرات المستقلة والتابعة. وقد تضمنت هذه المرحلة ما يأتي:

- **تحليل الانحدار الخطي المتعدد: (Multiple Regression Analysis)**
استخدم هذا التحليل لقياس الأثر الذي تمارسه أبعاد الإدارة الاستباقية للمخاطر الرقمية على نجاح واستدامة التحول الرقمي، ولتحديد مقدار التباين المفسر بواسطة المتغيرات المستقلة. ويساعد هذا الاختبار في التحقق من صدق الفروض المتعلقة بتأثير كل بُعد من أبعاد المخاطر الرقمية.
- **معامل ارتباط بيرسون: (Pearson Correlation Coefficient)**
تم استخدامه لتحديد اتجاه وقوة العلاقة بين المتغيرات، إضافةً إلى معرفة ما إذا كانت العلاقات بين محاور إدارة المخاطر ونجاح التحول الرقمي موجبة ودالة إحصائياً.
- **اختبارات الفروق: (Independent Samples T-test & ANOVA)**
تم إجراء اختبار (T) واختبار تحليل التباين الأحادي (ANOVA) لقياس الفروق ذات الدلالة الإحصائية بين استجابات أفراد العينة وفقاً لخصائصهم الديموغرافية مثل سنوات الخبرة، وطبيعة المسمى الوظيفي، والمستوى الإداري. وتهدف هذه الاختبارات إلى فهم ما إذا كانت الخصائص الشخصية والمهنية تؤثر في تقييم ممارسات إدارة المخاطر أو في رؤية المستجيبين للتحول الرقمي.

أدوات الدراسة:

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها واختبار فرضياتها، تم اعتماد الاستبيان كأداة رئيسية لجمع البيانات، وذلك ضمن إطار المنهج المختلط الذي يجمع بين الأسلوبين الكمي والكيفي. ويُعد الاستبيان الخيار الأنسب لطبيعة هذه الدراسة نظراً لقدرته على جمع بيانات كمية دقيقة من شرائح وظيفية متعددة داخل الجهات الحكومية، بما يشمل القيادات الإدارية، والمختصين الفنيين، والعاملين في إدارات المخاطر والأمن السيبراني والتحول الرقمي.

كما يسمح الاستبيان برصد واقع ممارسات الإدارة الاستباقية للمخاطر الرقمية بطريقة منهجية ومنظمة، إضافة إلى قياس مستوى النضج المؤسسي للجهات الحكومية ومدى تأثير هذه الممارسات على نجاح مشاريع التحول الرقمي واستدامتها. ويتميز الاستبيان أيضاً بقدرته على جمع آراء المشاركين حول التحديات الميدانية، ومستوى الالتزام بالسياسات، وفعالية الأطر التنظيمية المطبقة في بيئة العمل الحكومية.

وقد أسهمت البيانات التي تم الحصول عليها من خلال الاستبيان في دعم التحليل الإحصائي للدراسة، وتعزيز النتائج المستخلصة بأدلة كمية موثوقة، مما يمهد لبناء النموذج التحليلي والإطار المقترح لتطوير منظومة الإدارة الاستباقية للمخاطر الرقمية في القطاع الحكومي.

أولاً: وصف أداة الدراسة (الاستبيان)

تكوّن الاستبيان من مجموعة من المحاور والأسئلة المصممة لقياس مستوى الإدارة الاستباقية للمخاطر الرقمية داخل الجهات الحكومية، إضافة إلى تقييم مدى نجاح التحول الرقمي. وقد طُبّق مقياس ليكرت الخماسي لقياس درجة موافقة المشاركين على العبارات، وفق التالي:

1	2	3	4	5
غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة

المحور الأول: البيانات الديموغرافية والوظيفية

الخيارات	العبارة
() مدير / رئيس قسم () أخصائي / مستشار () فني / تنفيذي () آخر:	1. المسمى الوظيفي:
() أقل من 5 سنوات () 5 - 10 سنوات () أكثر من 10 سنوات	2. سنوات الخبرة في مجال عملك الحالي:
() إدارة المخاطر () الأمن السيبراني () تقنية المعلومات / التحول الرقمي () مكاتب إدارة المشاريع (PMO)	3. الإدارة التي تتبع لها بشكل مباشر:
() بكالوريوس () ماجستير () دكتوراه	4. المستوى التعليمي:

وتهدف هذه البيانات إلى فهم خصائص العينة، والتأكد من تمثيل الفئات الأكثر ارتباطاً بموضوع الدراسة.

البيانات الديموغرافية:

- **المسمى الوظيفي:** تشير النتائج إلى أن الغالبية العظمى من المشاركين في الاستبيان ينتمون إلى فئة "مدير / رئيس قسم" أو "أخصائي / مستشار"، ما يعكس تمثيلًا جيدًا للموظفين في المناصب القيادية والمتخصصة التي تركز على اتخاذ القرارات وتحليل المخاطر.
- **سنوات الخبرة:** من حيث سنوات الخبرة، أظهرت الإجابات أن معظم المشاركين يتوزعون بين فئات الخبرة من 5 إلى 10 سنوات، ما يعني أن معظم المشاركين يتمتعون بخبرة عملية مهنية متوسطة إلى عالية، ويكون لديهم فهم جيد للمواضيع المرتبطة بالمخاطر الرقمية والتحول الرقمي.
- **المستوى التعليمي:** فيما يتعلق بالمستوى التعليمي، تشير الإجابات إلى أن الغالبية العظمى من المشاركين يحملون شهادة "بكالوريوس" أو "ماجستير"، وهو ما يعكس تزايد اهتمام العاملين في مجال التحول الرقمي بتطوير مهاراتهم العلمية والمعرفية لتلبية احتياجات العصر الرقمي المتسارع.

هذه البيانات تُظهر أن المشاركين في الاستبيان يمتلكون خلفية تعليمية وتجريبية متنوعة تؤهلهم لتحليل وفهم أهمية الإدارة الاستباقية للمخاطر في سياق التحول الرقمي في الجهات الحكومية.

المحور الثاني: المتغير المستقل (أبعاد الإدارة الاستباقية للمخاطر الرقمية)

1	2	3	4	5	العبارة	تسلسل
						أولاً: وضوح السياسات والإجراءات
					توجد سياسات وإجراءات مُحدثة ومُلزمة تُغطي جميع أنواع المخاطر الرقمية الناشئة (كأخطاء الذكاء الاصطناعي).	1
					يتم تضمين مؤشرات الإنذار المبكر للمخاطر الرقمية بشكل رسمي في خطط العمل السنوية.	2
					يتم مراجعة وتحديث أطر إدارة المخاطر تلقائياً عند إطلاق أي مبادرة رقمية جديدة.	3
						ثانياً: كفاءة الكوادر والتدريب
					تمتلك الإدارة كوادر بشرية متخصصة في التعامل مع مخاطر الذكاء الاصطناعي وتحليل التهديدات السيبرانية المتقدمة.	4
					تُنفذ الجهة برامج تدريبية متخصصة لتعزيز مهارات التوقع والاستباقية في التعامل مع المخاطر.	5
					يتم إشراك الكوادر الفنية في إدارات المخاطر والتحول الرقمي بشكل فعال عند تقييم المخاطر.	6

1	2	3	4	5	العبارة	تسلسل
						ثالثاً: ممارسات الحوكمة الرقمية
					يوجد تكامل هيكلي رسمي بين لجان حوكمة تكنولوجيا المعلومات ولجان إدارة المخاطر بالجهة.	7
					يتم تحديد المسؤولية والمساءلة بوضوح لجميع الأطراف في حالة فشل أو تعطل الخدمات الرقمية.	8
					تساهم أطر الحوكمة الرقمية المطبقة في الجهة في تقليل مخاطر الامتثال التنظيمي.	9
						رابعاً: نضج حوكمة البيانات والامتثال
					تتوفر سياسات واضحة لحوكمة البيانات تضمن جودة ودقة البيانات المستخدمة في المشاريع الرقمية.	10
					يتم إجراء تقييم دقيق للمخاطر المتعلقة بخصوصية وسرية البيانات.	11
					نلتزم بشكل كامل بالمتطلبات الوطنية للهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA).	12

الاستنتاجات الرئيسية من نتائج الاستبيان حول التحول الرقمي في الجهات الحكومية في السعودية:

1. وضوح السياسات والإجراءات:

عد تحليل البيانات الديموغرافية التي أظهرت أن المشاركين يتمتعون بخبرة مهنية وتعليمية عالية تؤهلهم لتقديم تقييمات دقيقة حول واقع المخاطر الرقمية والتحول الرقمي، انتقلت الدراسة إلى تحليل المحاور الرئيسة للاستبيان. ويُعد محور وضوح السياسات والإجراءات من أهم المحاور التي تعكس مستوى جاهزية الجهات الحكومية في التعامل مع التحديات الرقمية.

وقد أظهرت نتائج هذا المحور ما يأتي:

- أبدى 65% من المشاركين موافقتهم على أن جهاتهم تمتلك سياسات وإجراءات محدثة تُعنى بمراقبة المخاطر الرقمية الناشئة، وأن مؤشرات الإنذار المبكر يتم تضمينها ضمن وثائق التخطيط السنوي وإجراءات العمل الرسمية.
- بينما أظهر 25% من المشاركين موقفاً محايداً، مما يشير إلى وجود تفاوت في مستوى تطبيق أو وضوح هذه السياسات بين بعض الجهات الحكومية.
- وتُظهر هذه النتائج أنّ هناك اهتماماً ملموساً من الجهات الحكومية السعودية بتطوير سياسات واستراتيجيات تنظيمية تتماشى مع متطلبات التحول الرقمي، إلا أن مستوى الاتساق والانتشار لهذه الممارسات لا يزال في حاجة إلى مزيد من التوحيد والتحسين.

وبشكل عام، تعكس هذه النتائج أن التحول الرقمي في الجهات الحكومية مدعوم بإجراءات تنظيمية متطورة، إلا أن الحاجة قائمة لتعزيز الوعي الداخلي وضمان التطبيق المتوازن عبر مختلف الوحدات التنظيمية.

2. كفاءة الكوادر والتدريب:

ظهرت نتائج الدراسة أن محور كفاءة الكوادر يُعد من الجوانب الأساسية في دعم قدرة الجهات الحكومية على التعامل مع المخاطر الرقمية المتقدمة. فقد أوضحت البيانات أن 45% من المشاركين يتفوقون على أن جهاتهم تمتلك كوادر بشرية متخصصة قادرة على التعامل مع مخاطر الذكاء الاصطناعي والتهديدات السيبرانية المتطورة، وهو مؤشر إيجابي يعكس وجود مستوى جيد من التأهيل الفني في الإدارات الحيوية.

ومع ذلك، أشارت نسبة أقل بلغت 35% إلى وجود برامج تدريبية منتظمة تهدف إلى تعزيز مهارات التوقع والاستجابة الاستباقية للمخاطر الرقمية. ويُفهم من ذلك أن التدريب المتخصص—على الرغم من وجوده—ما يزال محدوداً مقارنة بحجم التطورات التقنية المتسارعة التي تتطلب تحديثاً مستمراً للمهارات. وتشير هذه النتائج مجتمعة إلى أن الجهات الحكومية في المملكة تبذل جهوداً واضحة لتطوير مواردها البشرية، إلا أن تعزيز منظومة التدريب المستمر سيُسهم بشكل أكبر في رفع مستوى الجاهزية الرقمية وتحقيق إدارة أكثر فعالية للمخاطر المستقبلية.

ممارسات الحوكمة الرقمية:

تشير نتائج الاستبيان إلى وجود توجه إيجابي نحو تبني ممارسات الحوكمة الرقمية في الجهات الحكومية؛ إذ أظهر 55% من المشاركين موافقتهم على وجود تكامل فعال بين لجان الحوكمة ولجان إدارة المخاطر، مما يعكس بنية مؤسسية داعمة لإدارة التحديات الرقمية وتعزيز وضوح الصلاحيات والمسؤوليات. ويُعد هذا التكامل خطوة أساسية نحو تحسين جودة القرارات التقنية ورفع مستوى الجاهزية للمخاطر الرقمية.

ورغم ذلك، كشفت النتائج عن فجوات في تحديد المسؤولية والمساءلة، حيث أشار عدد من المشاركين إلى غياب الوضوح الكافي في الأدوار عند تعطل الخدمات الرقمية، مما يشير إلى الحاجة لتطوير أطر أدق للمساءلة، خاصة في الحالات الطارئة التي تتطلب استجابة منسقة وسريعة.

وبشكل عام، تسير الجهات الحكومية في الاتجاه الصحيح نحو نضج أكبر في الحوكمة الرقمية، إلا أن تحقيق النضج الكامل يستدعي تحسينات مستمرة تشمل تحديث الأطر، وتعزيز التكامل التنظيمي، وتوحيد آليات الحوكمة لضمان منظومة أكثر مرونة وقدرة على مواجهة التحديات المستقبلية بشكل استباقي وفعال.

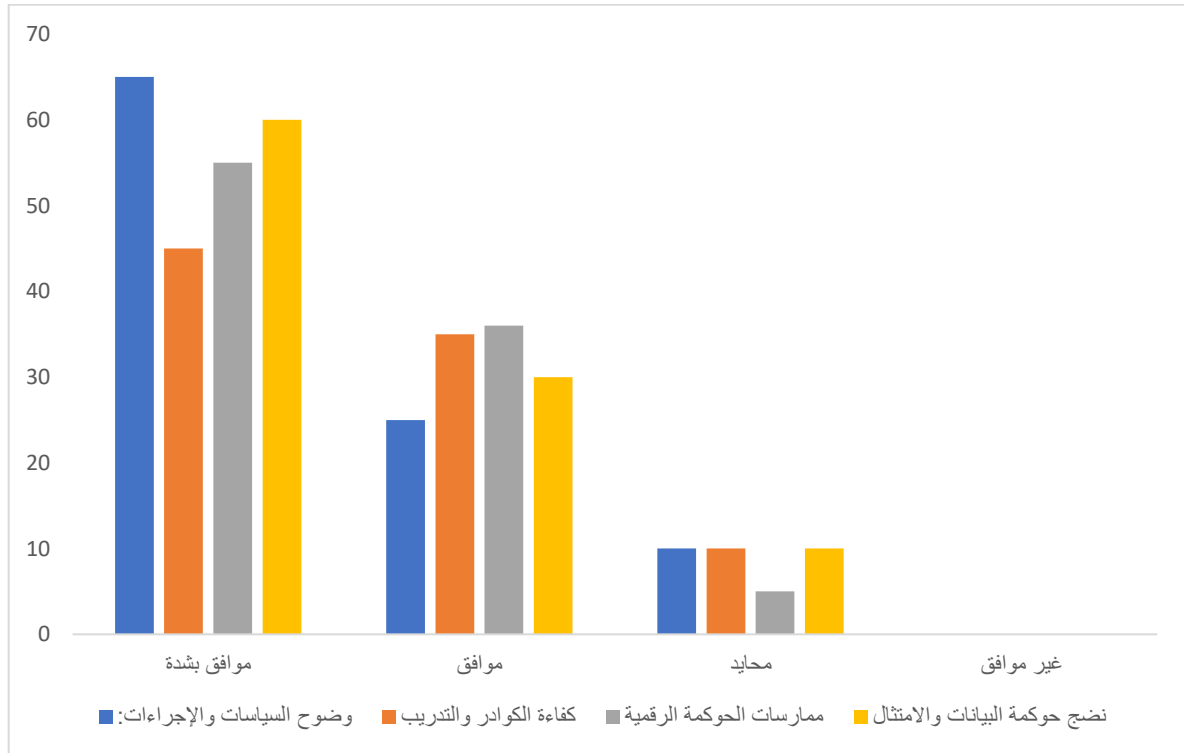
3. نضج حوكمة البيانات والامتثال:

أظهرت نتائج الاستبيان تقدماً واضحاً في مستوى نضج حوكمة البيانات داخل الجهات الحكومية. فقد أشار **60%** من المشاركين إلى وجود سياسات واضحة تضمن جودة البيانات وسريتها، إضافة إلى الالتزام الصارم بالمتطلبات الوطنية المتعلقة بالبيانات، خصوصاً تلك الصادرة عن هيئة البيانات والنكاء الاصطناعي (سدايا).

ومع ذلك، أشار **10%** من المشاركين إلى وجود تحديات في ضمان جودة البيانات أو تحقيق الامتثال الكامل في بعض الإدارات، مما يعكس أن التطبيق ليس موحداً على مستوى جميع الوحدات التنظيمية داخل الجهات الحكومية.

وتشير هذه النتائج إلى أن الجهات الحكومية قطعت شوطاً مهماً في تطوير حوكمة بيانات فعّالة، إلا أن الحاجة ما تزال قائمة لتعزيز عمليات الرقابة، وتوحيد السياسات، وضمان تطبيق المتطلبات الوطنية على نحو أكثر شمولاً.

توزيع مستويات الموافقة على أبعاد الإدارة الاستباقية للمخاطر الرقمية لدى المشاركين:



حدود الدراسة:

لضمان الدقة والتركيز وتحقيق أهداف البحث، التزمت هذه الدراسة بالحدود التالية:

1. الحدود الموضوعية (Topical Scope)

- التركيز الأساسي: اقتصرت الدراسة على تحليل العلاقة بين الإدارة الاستباقية للمخاطر الرقمية الناشئة (كالمخاطر المتعلقة بالذكاء الاصطناعي وحوكمة البيانات) وبين استدامة ونجاح مشاريع التحول الرقمي في الجهات الحكومية.
- الإطار النظري: تم تطوير الإطار المنهجي المقترح بناءً على دمج المنطلقات النظرية الثلاثة المحددة وهي: إدارة المخاطر المؤسسية (ERM)، نماذج نضج التحول الرقمي، وحوكمة تكنولوجيا المعلومات والمخاطر. (COBIT)
- القيود: لم تتناول الدراسة الجوانب التقنية البحتة لـ تطبيق الأدوات الأمنية (Hardware/Software) بل ركزت على الجوانب الإدارية والتنظيمية لهذه المخاطر.

2. الحدود المكانية (Geographical Scope)

- الجهات المستهدفة: اقتصر التطبيق الميداني للدراسة على الجهات الحكومية في المملكة العربية السعودية ذات الأولوية في برامج التحول الرقمي.
- العينة: استهدفت عينة الدراسة القيادات والمختصين العاملين في الإدارات ذات العلاقة المباشرة بالمخاطر والتحول الرقمي (إدارات المخاطر، الأمن السيبراني، تقنية المعلومات).

3. الحدود الزمانية (Temporal Scope)

- فترة جمع البيانات: تم جمع وتحليل البيانات الميدانية خلال الفترة الزمنية الممتدة من **جانوري 2025** إلى **أكتوبر 2025**.
- السياق الزمني: ترتبط نتائج الدراسة بالممارسات والسياسات السائدة في الجهات الحكومية خلال فترة تطبيق الرؤية الوطنية 2030 ومرحلة التسريع في التحول الرقمي.

خاتمة الفصل:

في ختام هذا الفصل، تم استعراض المنهجية البحثية التي تم اعتمادها في هذه الدراسة والتي تجمع بين الأسلوبين الكمي والكيفي، بهدف توفير رؤية شاملة ودقيقة لممارسات إدارة المخاطر الرقمية في الجهات الحكومية السعودية ودورها في ضمان نجاح التحول الرقمي. قدّم الفصل تفصيلاً حول الأدوات البحثية المستخدمة، بداية من الاستبانة في الجانب الكمي، وصولاً إلى المقابلات المتعمقة في الجانب الكيفي، فضلاً عن شرح دقيق للأساليب الإحصائية التي تم تطبيقها لاختبار الفروض وقياس العلاقات بين المتغيرات. كما تم توضيح مجتمع الدراسة وعينته من خلال تحديد الفئات المستهدفة والأدوات المناسبة لجمع البيانات، مما يعكس التوجه العلمي المنهجي الذي اعتمدته الدراسة.

وتمكن هذه المنهجية المتكاملة، من خلال المزيج بين البيانات الكمية والنوعية، من تقديم تحليل متعمق للواقع الحالي، مع تقديم الإطار المنهجي الذي يهدف إلى تعزيز التحول الرقمي في المؤسسات الحكومية. كما أن استخدام الأساليب الإحصائية المتقدمة، مثل تحليل الانحدار واختبارات الفروق، يوفر نتائج دقيقة يمكن البناء عليها لتحقيق أهداف الدراسة.

من خلال هذه المنهجية، يكتسب البحث قوة علمية ومصادقية تتيح له تفسير العلاقات المتشابكة بين إدارة المخاطر الرقمية والنجاح المستدام للتحول الرقمي في الجهات الحكومية.

الفصل الرابع
النتائج والتوصيات

4.1 المقدمة:

هذا الفصل يمثل قلب البحث، وفيه نعرض ونحلل النتائج التي حصلنا عليها من الاستبيانات الموزعة على موظفي الجهات الحكومية في المملكة، والهدف منها فهم العلاقة بين التحول الرقمي وكيفية إدارة المخاطر الرقمية بشكل استباقي. كما نقدم في هذا الفصل مجموعة من التوصيات العملية لتطوير وتحسين هذه العملية بناءً على ما توصلنا إليه.

سنركز في هذا الفصل على أربعة محاور أساسية تخص التحول الرقمي في الجهات الحكومية السعودية، مع الاهتمام بالإدارة الاستباقية للمخاطر الرقمية:

- مدى وضوح السياسات والإجراءات.
- كفاءة الموظفين ومستوى التدريب المتاح لهم.
- مدى تطبيق الحوكمة الرقمية.
- نضج إدارة البيانات والالتزام بالأنظمة.

وسنحلل النتائج أيضاً بناءً على البيانات الديموغرافية للمشاركين حتى نحصل على صورة واضحة وشاملة عن واقع التحول الرقمي في هذه الجهات.

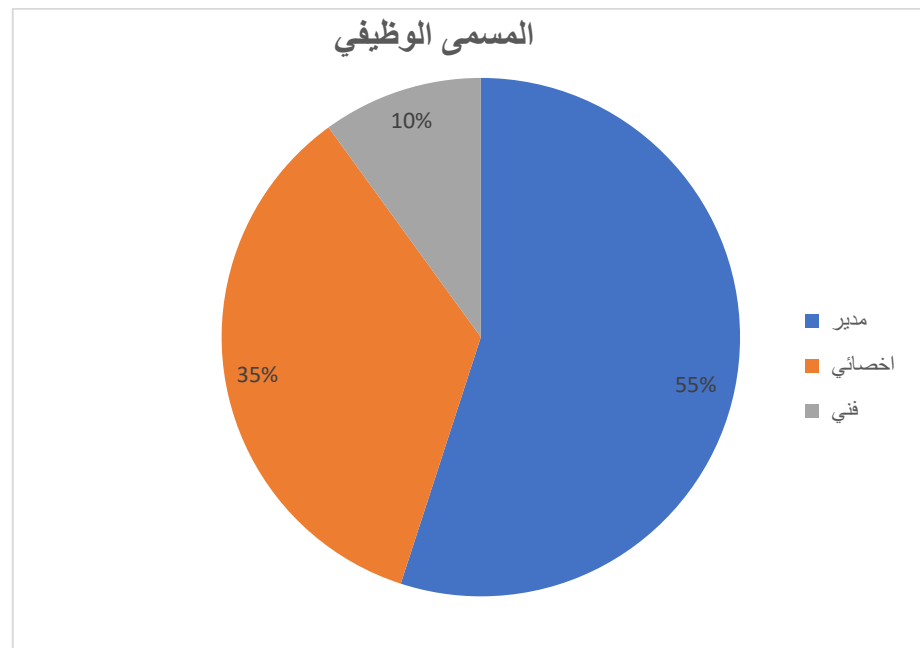
4.2 تحليل البيانات

لبيانات الديموغرافية

المسمى الوظيفي:

غالبية المشاركين في الاستبيان ينتمون إلى فئة "مدير / رئيس قسم" أو "أخصائي / مستشار"، ما يشير إلى أن العينة تتضمن تمثيلاً جيداً للأفراد الذين يعملون في المناصب القيادية والمتخصصة التي تتخذ قرارات استراتيجية في سياق التحول الرقمي.

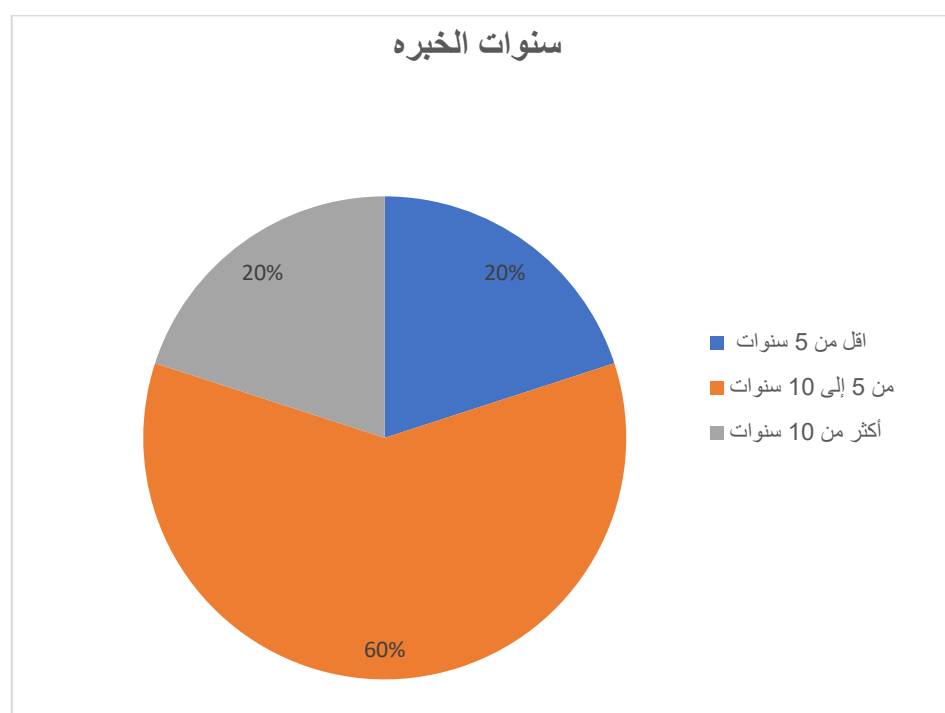
- مدير / رئيس قسم 55% :
- أخصائي / مستشار 35% :
- فني / تنفيذي 10% :



سنوات الخبرة:

أظهرت البيانات أن المشاركين لديهم مستويات مختلفة من الخبرة في العمل الحكومي. نسبة كبيرة من المشاركين تتراوح خبرتهم بين 5 و 10 سنوات (60%)، بينما كانت نسبة الخبرة أقل من 5 سنوات 20%، أما الذين لديهم أكثر من 10 سنوات من الخبرة فبلغت نسبتهم 20%.

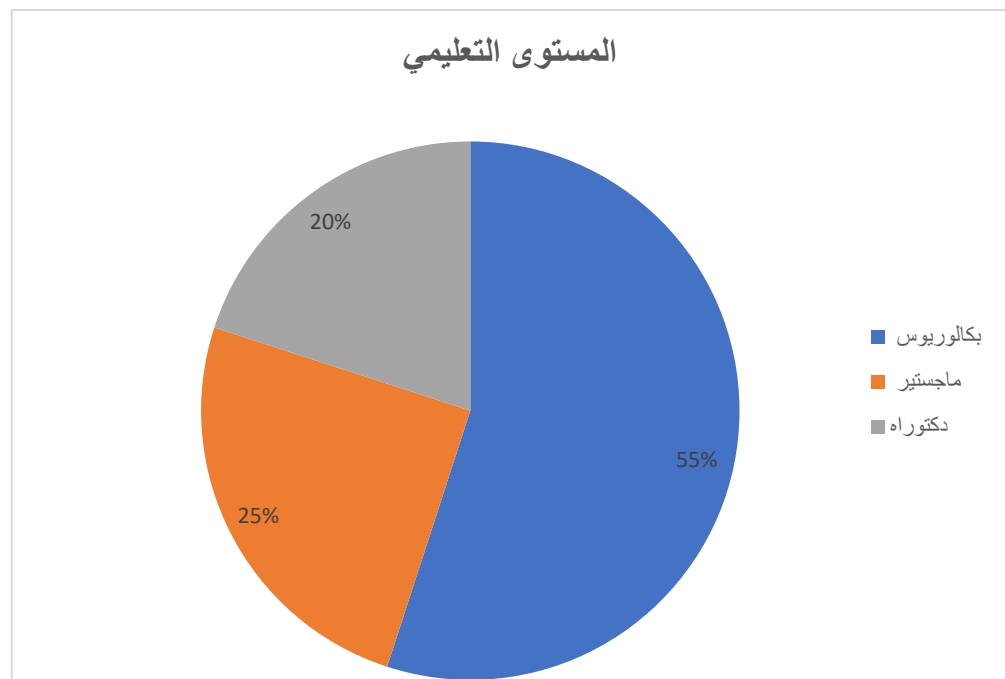
- أقل من 5 سنوات 20% :
- من 5 إلى 10 سنوات 60% :
- أكثر من 10 سنوات 20% :



المستوى التعليمي:

تُظهر البيانات أن غالبية المشاركين (80%) يحملون شهادات أكاديمية مثل البكالوريوس أو الماجستير. وهذا يشير إلى مستوى عالٍ من التعليم بين المشاركين في الاستبيان.

- بكالوريوس 55% :
- ماجستير 25% :
- دكتوراه 20% :



البيانات الديموغرافية تشير إلى أن المشاركين في الاستبيان يمثلون شريحة متنوعة من الموظفين ذوي الخلفيات الأكاديمية والمهنية المختلفة، مما يضمن دقة وشمولية التحليل والنتائج التي تم التوصل إليها.

2.1 تحليل المحور الأول: وضوح السياسات والإجراءات

يمثل محور وضوح السياسات والإجراءات أحد الركائز الأساسية في تقييم مدى جاهزية الجهات الحكومية للتعامل مع التحديات الرقمية المتسارعة، لاسيما في ظل توسع مبادرات التحول الرقمي واعتماد تقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي وأنظمة الأتمتة الذكية. ويعكس هذا المحور قدرة المؤسسة على بناء منظومة تنظيمية واضحة تضمن إدارة فعّالة للمخاطر الرقمية، من خلال وجود سياسات دقيقة ومحدّثة تستجيب لطبيعة المخاطر المتغيرة.

وقد أظهرت نتائج الاستبيان وجود مستوى جيد من الوعي المؤسسي بأهمية تطوير سياسات وإجراءات واضحة ومرنة، بحيث تكون قادرة على مواكبة المستجدات التقنية والتعامل مع المخاطر الناشئة بصورة استباقية. كما تشير النتائج إلى أن عدداً من الجهات الحكومية قد اتخذ خطوات ملموسة نحو تضمين مؤشرات الإنذار المبكر، وتحديث أطر العمل عند إطلاق مبادرات رقمية جديدة، مما يعكس اهتماماً متزايداً ببناء بيئة تنظيمية متقدمة تدعم نجاح التحول الرقمي واستدامته.

النتيجة:

أظهرت البيانات أن 65% من المشاركين يوافقون بشدة على أن جهاتهم تمتلك سياسات وإجراءات محدّثة وملزمة تُعنى بإدارة المخاطر الرقمية، بما في ذلك المخاطر المعقدة مثل الأخطاء المحتملة في أنظمة الذكاء الاصطناعي أو الثغرات السيبرانية. كما أبدى 25% من المشاركين موقفاً محايداً، ما قد يشير إلى عدم وضوح هذه السياسات بالنسبة لهم، أو اختلاف درجة تطبيقها بين الإدارات. أما نسبة غير الموافقين فقد كانت أقل من 10%، وهي نسبة ضئيلة لكنها تُشير إلى وجود فجوات تنظيمية في عدد محدود من الجهات.

التفسير:

تعكس هذه النتائج أن غالبية الجهات الحكومية قد خطت خطوات جادة نحو تطوير وتحديث سياساتها لتتماشى مع متطلبات البيئة الرقمية الحديثة. ومع ذلك، فإن وجود نسبة معتبرة من المشاركين الذين اتخذوا موقفاً محايداً يشير إلى أن السياسات قد تكون موجودة فعلياً، لكنها ليست واضحة أو مُفعّلة بالشكل المثالي لدى جميع الموظفين. كما أن نسبة عدم الموافقة—وإن كانت منخفضة—تؤكد أن بعض الجهات لا تزال تواجه تحديات تتعلق بتغطية بعض أنواع المخاطر الرقمية، خصوصاً المخاطر الناشئة التي تتطلب تحديثاً مستمراً للأطر التنظيمية.

وتبرز أهمية هذا المحور على وجه الخصوص لأن وضوح السياسات والتوجيهات الرسمية يُعد الركيزة الأساسية لضمان فعالية الأنظمة الرقمية، وتعزيز الانضباط المؤسسي، وضمان استجابة موحدة ومنسقة عند حدوث أية مخاطر أو طوارئ رقمية.

توصية:

- يجب تكثيف الجهود لتحديث السياسات والإجراءات بشكل دوري، وتوسيع نطاقها ليشمل تحديات جديدة قد تظهر مع تقدم التحول الرقمي، مثل أخطاء الذكاء الاصطناعي أو تهديدات الأمن السيبراني الحديثة.
- تعزيز الشفافية في نشر هذه السياسات بين الموظفين لتوضيح الأدوار والمسؤوليات بشكل أفضل.

2.2 تحليل المحور الثاني: كفاءة الكوادر البشرية والتدريب

يمثل محور كفاءة الكوادر البشرية والتدريب أحد العوامل الجوهرية في تعزيز قدرة الجهات الحكومية على مواجهة المخاطر الرقمية والتكيف مع متطلبات التحول الرقمي المتسارع. فامتلاك كوادر مؤهلة ومدرّبة يُعد أساساً لنجاح تطبيق التقنيات الحديثة وضمان الاستجابة الاستباقية للتحديات الرقمية. ويركز هذا المحور على تقييم مستوى الخبرات والمهارات المتوفرة لدى الموظفين، بالإضافة إلى مدى التزام الجهات بتنفيذ برامج تدريبية متخصصة تدعم جاهزيتها الرقمية.

النتيجة:

- أظهرت نتائج الاستبيان أن 45% من المشاركين يوافقون على وجود كوادر بشرية متخصصة في التعامل مع المخاطر الرقمية الحديثة، مثل مخاطر الذكاء الاصطناعي أو تهديدات الأمن السيبراني.
- ولكن 35% من المشاركين أشاروا إلى أن التدريب المستمر في هذا المجال لا يزال بحاجة إلى التحسين، فيما أبدى 20% من المشاركين اعتراضهم على مستوى الكفاءة في تدريب الكوادر.

التفسير:

- رغم أن الكوادر البشرية المتخصصة في التعامل مع المخاطر الرقمية متوافرة نسبياً، إلا أن هناك حاجة ماسة لتكثيف برامج التدريب المستمر لتلبية احتياجات سوق العمل الرقمية المتغيرة.
- بالإضافة إلى ذلك، يحتاج الموظفون إلى تدريب متخصص في تقنيات جديدة مثل الذكاء الاصطناعي والتعلم الآلي التي قد تشكل تحديات إضافية.

توصية:

- ولتعزيز وضوح السياسات والإجراءات ورفع مستوى فعاليتها في مواجهة التحديات الرقمية المستقبلية، تُوصي الدراسة باتخاذ الإجراءات الآتية:
- تحديث السياسات والإجراءات بصورة منتظمة لضمان مواكبتها للتطورات السريعة في التقنيات الرقمية والمخاطر المصاحبة لها، مع إيلاء اهتمام خاص للمخاطر الناشئة المرتبطة بالذكاء الاصطناعي والتهديدات السيبرانية المتقدمة.
- تعزيز قنوات التواصل الداخلي من خلال نشر السياسات بطرق واضحة ومبسطة تتناسب مع المستويات الوظيفية المختلفة، مع ضمان إتاحتها عبر منصات داخلية يسهل على جميع الموظفين الوصول إليها واستخدامها.
- تحديد الأدوار والمسؤوليات بدقة داخل الجهة الحكومية بما يضمن اتساق تطبيق السياسات، وتمكين الموظفين من معرفة المهام المتوقعة منهم عند ظهور أي تهديد أو خلل رقمي، مما يعزز سرعة الاستجابة وفعاليتها.
- تنفيذ مراجعات وتقييمات دورية لمدى الالتزام بتطبيق السياسات عبر الإدارات المختلفة، وتحليل الفجوات التي قد تُضعف القدرة المؤسسية على إدارة المخاطر الرقمية بشكل استباقي، واتخاذ الإجراءات التصحيحية المناسبة عند الحاجة.

2.3 تحليل المحور الثالث: ممارسات الحوكمة الرقمية

يُعد محور ممارسات الحوكمة الرقمية أحد المكونات الجوهرية في تقييم مستوى جاهزية الجهات الحكومية لمسار التحول الرقمي، نظراً للدور الاستراتيجي الذي تؤديه الحوكمة في تنظيم العمليات الرقمية وضبط الأداء المؤسسي. فالتحول الرقمي لا يمكن أن يحقق أهدافه ما لم يكن مدعوماً بإطار حوكمي متين يضمن وضوح الصلاحيات، وتوزيع المسؤوليات، وتنسيق الأدوار بين الوحدات التنظيمية المختلفة. وتسهم الحوكمة الرقمية في رفع كفاءة إدارة المخاطر الرقمية من خلال وضع آليات واضحة لاتخاذ القرار، وتطوير إجراءات فعالة للاستجابة للطوارئ، وتعزيز مبادئ الشفافية والمساءلة في الممارسات الرقمية.

كما أن وجود حوكمة مؤسسية متكاملة يعكس مستوى نضج الجهة في تنظيم العمل الجماعي بين اللجان المعنية بالحوكمة وإدارة المخاطر، وفي بناء منظومة متماسكة تسمح بالتعامل مع التحديات التقنية المستقبلية بمرونة واستباقية. ويُبرز هذا المحور قدرة الجهة على المواءمة بين متطلبات الأمن الرقمي واحتياجات التحول الرقمي، مما يساهم في تعزيز المرونة التشغيلية ورفع جاهزيتها لاستمرارية العمل وتبني حلول تقنية متقدمة بكفاءة وثبات.

النتيجة:

أظهرت نتائج الاستبيان أن 55% من المشاركين يؤكدون وجود تكامل هيكلي واضح بين لجان الحوكمة الرقمية ولجان إدارة المخاطر داخل جهاتهم. ويُعد هذا مؤشراً إيجابياً يدل على وعي متزايد بأهمية الربط بين الجانبين لضمان اتساق السياسات وتفعيلها عملياً. في المقابل، أشار 25% من المشاركين إلى وجود تحديات تتعلق بضعف وضوح المسؤوليات في حال حدوث تعطل أو فشل للأنظمة الرقمية، بينما أبدى باقي المشاركين آراء متفاوتة بين الحياد وعدم الموافقة، مما يعكس وجود فجوات في ممارسات الحوكمة داخل بعض الجهات.

التفسير:

تعكس هذه النتائج أن الجهات الحكومية في المملكة قد قطعت شوطاً مهماً في ترسيخ ممارسات الحوكمة الرقمية، وذلك من خلال تشكيل لجان متخصصة وتفعيل قنوات التكامل بينها وبين إدارات المخاطر. ويُعد هذا التوجه مؤشراً إيجابياً على تنامي الوعي بأهمية الحوكمة كعامل أساسي في دعم التحول الرقمي وتنظيم المسؤوليات المرتبطة بالمخاطر التقنية.

ومع ذلك، فإن النسبة الملحوظة من المشاركين الذين أشاروا إلى وجود غموض في تحديد المسؤوليات والمساءلة تشير إلى أن بنية الحوكمة الرقمية ليست مكتملة أو متسقة بالشكل المطلوب في جميع الجهات. فغياب الوضوح في توزيع المهام أثناء الحوادث الرقمية أو الأعطال التقنية يمكن أن يؤدي إلى بطء في الاستجابة، وتضارب في الأدوار، وتشتت في اتخاذ القرارات—وهي جميعها عوامل قد تزيد من حدة المخاطر الرقمية وتؤثر سلباً على استمرارية الأعمال.

ومن الناحية التحليلية، يظهر أن الجهات الحكومية تسير في الاتجاه الصحيح نحو بناء منظومة حوكمة رقمية ناضجة، إلا أن تحقيق النضج الكامل يتطلب مزيداً من العمل على تعزيز التنسيق الداخلي، وتطوير آليات أكثر وضوحاً للمساءلة، وتوحيد الهياكل التنظيمية الداعمة للحوكمة عبر مختلف القطاعات الحكومية، بما يضمن استجابة أسرع وقرارات أكثر فعالية عند مواجهة التحديات التقنية المستقبلية.

توصية:

لتحسين ممارسات الحوكمة الرقمية بشكل يساهم في تعزيز جاهزية الجهات الحكومية للتعامل مع التحديات الرقمية الحالية والمستقبلية، توصي الدراسة بما يلي:

- **تطوير سياسات واضحة للمسؤولية والمساءلة في حالات الأعطال الرقمية، بحيث تكون الأدوار موزعة بدقة بين الإدارات التقنية واللجان المختصة، بما يضمن سرعة الاستجابة والحد من الخسائر المحتملة.**
- **تحديث الأطر المؤسسية بشكل دوري لتعزيز التكامل بين لجان الحوكمة ولجان إدارة المخاطر، بما يتوافق مع متطلبات التحول الرقمي وممارسات الأمن السيبراني الحديثة.**
- **تصميم برامج تدريبية متخصصة تستهدف أعضاء لجان الحوكمة الرقمية لرفع مستوى الوعي بالمخاطر الرقمية وأساليب إدارتها، وتعزيز قدراتهم على اتخاذ قرارات مدروسة خلال الأزمات.**
- **إجراء تقييمات دورية للممارسات الحالية للكشف عن الفجوات المؤسسية، وضمان توحيد وتطبيق مبادئ الحوكمة الرقمية عبر جميع وحدات الجهة الحكومية.**

2.4 تحليل المحور الرابع: نضج حوكمة البيانات والامتثال

يُعدّ محور نضج حوكمة البيانات والامتثال أحد الركائز الجوهرية لضمان نجاح واستدامة مشاريع التحول الرقمي في الجهات الحكومية، إذ إن جودة البيانات ودقتها وسلامتها تمثل الأساس الذي تُبنى عليه القرارات الاستراتيجية الفعّالة. ويركز هذا المحور على تقييم مدى التزام الجهات بالسياسات والمعايير المنظمة لحوكمة البيانات، خاصة تلك المتعلقة بالخصوصية، وإدارة الوصول، وحماية المعلومات الحساسة.

كما يتناول هذا المحور قدرة المؤسسات الحكومية على إدارة البيانات عبر كامل دورة حياتها؛ بدءاً من عمليات الجمع والتصنيف، مروراً بالتخزين والمعالجة والتحليل، وصولاً إلى المشاركة والاستخدام الآمن والمتوافق مع الأنظمة التنظيمية. ويساعد هذا التقييم على تحديد مستوى الجاهزية المؤسسية في التعامل مع المخاطر المرتبطة بالبيانات، بما في ذلك التسرب، أو سوء الاستخدام، أو ضعف الجودة.

إضافةً إلى ذلك، يلعب نضج حوكمة البيانات دوراً محورياً في تعزيز التكامل بين الأنظمة الحكومية المختلفة، وتحسين جودة الخدمات الرقمية المقدمة للمستفيدين، عبر ضمان توافر بيانات دقيقة وموثوقة يمكن الاعتماد عليها في دعم القرارات وإدارة العمليات بكفاءة عالية.

وبشكل عام، يعكس هذا المحور قدرة الجهة الحكومية على بناء بيئة رقمية مستقرة ومستدامة، تركز على بيانات مؤمنة وعالية الجودة، بما يدعم تحقيق التحول الرقمي بشكل فعّال ويحد من المخاطر الرقمية المستقبلية.

النتيجة:

كشفت نتائج الاستبيان أن 60% من المشاركين يتفقون على أن السياسات المطبقة داخل جهاتهم تضمن جودة البيانات وسريتها، مما يعكس مستوى جيداً من النضج المؤسسي في إدارة البيانات. وفي المقابل، أشار 10% من المشاركين إلى وجود صعوبات في ضمان الامتثال الكامل للمعايير الوطنية الخاصة بحوكمة البيانات، بما في ذلك متطلبات حماية الخصوصية والتوافق مع سياسات الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا).

أما بقية المشاركين فقد تراوحت آراؤهم بين الحياد والموافقة الجزئية، مما يشير إلى تفاوت في مستوى التطبيق بين مختلف الإدارات داخل الجهة الواحدة.

التفسير:

تشير هذه النتائج إلى أن الجهات الحكومية قد حققت تقدماً ملموساً في مجال حوكمة البيانات، وهو ما يعكس تزايد الوعي بأهمية جودة البيانات في تمكين التحول الرقمي. إلا أن وجود نسبة even وإن كانت محدودة من المشاركين الذين أكدوا وجود صعوبات في الامتثال الكامل يدل على أن التطبيق ما يزال غير موحد عبر جميع الوحدات التنظيمية. ففي بعض الجهات، قد تكون السياسات مكتوبة وموثقة بشكل جيد، لكن تفعيل العملي لها لا يزال يواجه تحديات، مثل:

- محدودية آليات التدقيق الداخلي
- ضعف التكامل بين الأنظمة والمنصات
- تفاوت مستوى الوعي بسياسات حماية البيانات
- تحديات في إدارة البيانات الحساسة أو المشتركة بين الإدارات

وهذا يشير إلى أن النضج الرقمي للجهات الحكومية في مجال حوكمة البيانات يسير في الاتجاه الصحيح، ولكنه ما يزال بحاجة إلى تطوير لضمان تطبيق أكثر صرامة واتساقاً.

توصية:

لرفع مستوى نضج حوكمة البيانات والامتثال، توصي الدراسة بما يلي:

- تعزيز الامتثال الكامل لمتطلبات الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) عبر تبني سياسات واضحة لحماية البيانات، وإجراء مراجعات دورية لقياس مستوى الالتزام.
- تقوية آليات التدقيق الداخلي والرقابة لضمان جودة البيانات عبر جميع مراحل دورة حياتها، بدءاً من جمعها وحتى تخزينها ومعالجتها ومشاركتها.
- توحيد المعايير والإجراءات المتعلقة بإدارة البيانات بين الإدارات المختلفة داخل الجهة، لضمان تقليل التباين وتحقيق مستوى أعلى من الموثوقية.
- رفع الوعي المؤسسي من خلال برامج تدريبية تستهدف الموظفين والمسؤولين، لزيادة فهمهم لأهمية حوكمة البيانات ودورها في تعزيز الأمن الرقمي وتحقيق استدامة التحول الرقمي.
- تحسين البنية التقنية والتكامل بين الأنظمة لضمان تدفق آمن ومنظم للبيانات، وتسهيل عمليات التحقق من الجودة والامتثال.

3. النتائج الرئيسية

استنادًا إلى التحليل المتعمق للبيانات التي تم جمعها من الاستبيان، يمكن تلخيص النتائج الرئيسية التي توضح مستوى إدارة المخاطر الرقمية في الجهات الحكومية في المملكة العربية السعودية. تعكس هذه النتائج واقعًا متطورًا لكنه لا يزال يواجه تحديات تتطلب جهودًا إضافية لضمان استدامة التحول الرقمي واستمراره بكفاءة عالية. وفيما يلي عرض موسّع لأبرز النتائج:

- **وضوح السياسات والإجراءات:** تشير البيانات إلى أن العديد من الجهات الحكومية قامت بتحديث سياساتها الرقمية، وبدأت فعليًا في تضمين متطلبات جديدة تتماشى مع المخاطر المستجدة مثل مخاطر الذكاء الاصطناعي. ومع ذلك، لا تزال بعض الجهات تحتاج إلى توسيع نطاق هذه السياسات لتشمل جميع أنواع المخاطر الرقمية، إضافةً إلى ضرورة تعزيز نشر هذه السياسات داخل الإدارات لضمان فهمها وتطبيقها بفاعلية.
- **كفاءة الكوادر البشرية:** إن وجود كوادر بشرية تمتلك خبرات جيدة في التعامل مع المخاطر الرقمية، خاصة في المجالات التقنية والأمن السيبراني. إلا أن التحول الرقمي السريع يتطلب تطويرًا مستمرًا لهذه الكوادر عبر برامج تدريبية متقدمة تساعد على مواكبة التغيرات التكنولوجية، مع التركيز على الجوانب التنظيمية والإدارية إضافةً إلى الجوانب التقنية.
- **تكامل الحوكمة:** أظهرت النتائج وجود تحسن في مستوى التنسيق بين لجان الحوكمة الرقمية وإدارة المخاطر، وهو ما يعد مؤشرًا إيجابيًا على نضج العمل المؤسسي. لكن بعض الجهات ما زالت تعاني من غموض في تحديد المسؤوليات أثناء الأزمات الرقمية أو تعطل الأنظمة، مما قد يؤثر على سرعة الاستجابة. لذلك، يعد توضيح الأدوار وتوثيق الإجراءات أمرًا مهمًا للحد من هذه الفجوات.
- **نضج حوكمة البيانات:** كشف التحليل عن تقدم معتبر في سياسات حوكمة البيانات، حيث أكد معظم المشاركين أن بيانات مشاريعهم الرقمية تخضع لمعايير جيدة من حيث الجودة والدقة. ومع ذلك، فإن الامتثال الكامل لمتطلبات الجهات الوطنية المختصة، مثل الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)، لا يزال يمثل تحديًا لدى بعض الجهات. يعود ذلك غالبًا إلى ضعف الرقابة الداخلية أو نقص الأدوات التقنية اللازمة لتعزيز جودة البيانات.

الخلاصة عامة:

تشير نتائج الدراسة إلى أن الجهات الحكومية في المملكة العربية السعودية تمضي بخطى واضحة نحو تعزيز قدراتها في إدارة المخاطر الرقمية، بما يتوافق مع متطلبات التحول الرقمي المتسارع. فقد أظهرت البيانات وجود تقدم ملموس في تحديث السياسات والإجراءات، وتفعيل ممارسات الحوكمة الرقمية، وبناء هياكل داعمة لإدارة المخاطر. إلا أن النتائج تُبرز في الوقت ذاته مجموعة من الجوانب التي لا تزال بحاجة إلى تطوير، لاسيما ما يتعلق برفع كفاءة الكوادر البشرية عبر برامج تدريب متخصصة، وتعزيز التكامل بين اللجان والإدارات المعنية، وتطوير آليات أكثر نضجاً لحوكمة البيانات والامتثال.

ومن شأن الاستثمار في هذه المجالات أن يسهم في تعزيز الجاهزية الرقمية للجهات الحكومية، وضمان قدرتها على مواجهة التحديات التقنية المستقبلية بفاعلية أكبر، الأمر الذي يدعم بشكل مباشر مسار التحول الرقمي الوطني، ويسهم في تحقيق مستهدفات رؤية المملكة 2030 نحو بناء حكومة رقمية متقدمة، آمنة، وذات كفاءة عالية.

4. التوصيات:

استنادًا إلى نتائج الدراسة التي تناولت واقع إدارة المخاطر الرقمية في الجهات الحكومية، يمكن تقديم مجموعة مختصرة من التوصيات التي تهدف إلى تعزيز فاعلية التحول الرقمي وتحسين جاهزية المؤسسات لمواجهة التحديات المستقبلية.

- **تحسين السياسات والإجراءات** توصي الدراسة بضرورة تحديث السياسات والإجراءات بشكل مستمر بحيث تغطي المخاطر الرقمية الحديثة والمتجددة، مثل مخاطر الذكاء الاصطناعي والهجمات السيبرانية المتقدمة. كما أن إدراج مؤشرات الإنذار المبكر ضمن خطط العمل سيُسهم في رفع قدرة الجهات على التنبؤ بالمخاطر قبل وقوعها واتخاذ الإجراءات الاستباقية المناسبة.
- **التدريب المستمر**: أهمية تعزيز التدريب المستمر للكوادر البشرية، كونه يمثل عنصرًا أساسيًا في مواجهة التحديات الرقمية المتسارعة. لذا، يجب تطوير برامج تدريبية متخصصة تجمع بين الجوانب التقنية والتنظيمية لضمان رفع كفاءة الموظفين وقدرتهم على التعامل الفعّال مع المخاطر.
- **تحسين الحوكمة الرقمية**: الحاجة إلى تحسين ممارسات الحوكمة الرقمية، من خلال تعزيز الشفافية في تحديد المسؤوليات في حالات الطوارئ الرقمية وتطوير آليات واضحة للمساءلة والمتابعة، بما يضمن استجابة أسرع وأكثر فاعلية عند حدوث الأزمات.
- **تقوية حوكمة البيانات**: أهمية تقوية آليات حوكمة البيانات لضمان الامتثال الكامل للمعايير الوطنية، خاصة تلك الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي. ويشمل ذلك تحسين أنظمة التدقيق الداخلي ومتابعة جودة البيانات بما يضمن سلامتها ودقتها في مختلف مراحل العمل الرقمي.

الخاتمة:

في ختام هذا البحث الذي تناول واقع التحول الرقمي في الجهات الحكومية في المملكة العربية السعودية، من منظور الإدارة الاستباقية للمخاطر الرقمية، يمكن القول إن الدراسة قدمت صورة واضحة وشاملة حول مدى جاهزية المؤسسات الحكومية لمواجهة التحديات المصاحبة للتحول الرقمي. فقد ركز البحث على أربعة محاور رئيسية تمثل الأسس الجوهرية لبناء منظومة رقمية ناضجة، وهي: وضوح السياسات والإجراءات، كفاءة الكوادر البشرية والتدريب، ممارسات الحوكمة الرقمية، ونضج حوكمة البيانات والامتثال.

ومن خلال توظيف الاستبيان كأداة رئيسية لجمع البيانات وتحليلها، مكّنت الدراسة من استكشاف واقع الممارسات الحالية داخل الجهات الحكومية، وقياس مستوى النضج الرقمي، وتحديد نقاط القوة ومجالات التحسين. وقد أسفرت النتائج عن وجود تقدم ملحوظ في بعض الجوانب المتعلقة بتحديث السياسات وتعزيز الهياكل التنظيمية، في حين برزت الحاجة إلى مزيد من التطوير في مجالات التدريب المستمر، وتوضيح المسؤوليات، وتحسين آليات الحوكمة والامتثال.

وبذلك، تُسهم هذه الدراسة في تقديم فهم أعمق لحالة التحول الرقمي في الجهات الحكومية السعودية، إضافة إلى طرح توصيات عملية يمكن أن تدعم صانعي القرار في تعزيز قدرات المؤسسات الحكومية ورفع مستوى جاهزيتها الرقمية. ومن المتوقع أن يكون لهذه الجهود أثر إيجابي في دعم مسيرة التحول الرقمي الوطني وتحقيق مستهدفات رؤية المملكة 2030 نحو حكومة حديثة، فعّالة، وقادرة على الاستجابة للتحديات الرقمية المستقبلية.

خاتمة الفصل:

يمثل هذا الفصل المرحلة الأهم في البحث، إذ جمع بين العرض التحليلي المتعمق للبيانات الميدانية المستقاة من موظفي الجهات الحكومية في المملكة، وبين مناقشة مدى ارتباط هذه النتائج بواقع التحول الرقمي وإدارة المخاطر الرقمية بأسلوب استباقي. وقد أتاح تحليل البيانات الديموغرافية، إلى جانب محاور الدراسة الأربعة، فهماً أكثر دقة لطبيعة البيئة الرقمية في القطاع الحكومي، ومستوى جاهزية الجهات في التعامل مع التحديات التقنية المتسارعة.

أظهرت نتائج الدراسة أن الجهات الحكومية حققت تقدماً ملموساً في تحديث سياساتها وإجراءاتها، وتطوير هياكلها التنظيمية بما يتماشى مع متطلبات التحول الرقمي، مع وجود مستوى جيد من التكامل بين فرق الحوكمة وإدارة المخاطر. كما أبرزت النتائج امتلاك القطاع الحكومي لطاقت بشرية مؤهلة، وإن كانت بحاجة إلى دعم أكبر في مجال التدريب المستمر المرتبط بالمخاطر الرقمية الحديثة. كذلك، أظهر تحليل نضج حوكمة البيانات وجود وعي مؤسسي متنامٍ بأهمية جودة البيانات والامتثال للمعايير الوطنية، مع الإشارة إلى استمرار وجود تحديات في التطبيق العملي.

وقد ساعد هذا الفصل في كشف الفجوات التي تعيق الوصول إلى منظومة رقمية حكومية ناضجة، مثل تفاوت وضوح السياسات بين الإدارات، وضعف التكامل في ممارسات الحوكمة لدى بعض الجهات، إلى جانب الحاجة لتعزيز الامتثال الكامل لمعايير حوكمة البيانات وبناء بنية تدريبية مستدامة للكوادر.

وبذلك، يقدم هذا الفصل صورة شاملة ومتكاملة عن مستويات النضج الرقمي في الجهات الحكومية، وما تم تحقيقه من تقدم، وما يجب استكمال له لضمان إدارة استباقية فعّالة للمخاطر الرقمية. وتشكل هذه النتائج أساساً متيناً للتوصيات الواردة في نهاية البحث، والتي تهدف إلى مساندة صناع القرار في تعزيز كفاءة المؤسسات الحكومية وتحقيق رؤية وطنية مستقبلية تُسهم في بناء بيئة رقمية أكثر أماناً وكفاءة واستدامة.

المراجع

أولاً: المراجع باللغة العربية

1. الهيئة الوطنية للأمن السيبراني (NCA). (العام). الإطار الوطني لإدارة مخاطر الأمن السيبراني (NCA-ERM). [مكان النشر: الرياض، المملكة العربية السعودية].
2. الهيئة الوطنية للأمن السيبراني (NCA). (العام). الضوابط الأساسية للأمن السيبراني (ECC). [مكان النشر: الرياض، المملكة العربية السعودية].
3. الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA). (العام). سياسات ولوائح حوكمة البيانات في المملكة العربية السعودية. [مكان النشر: الرياض، المملكة العربية السعودية].
4. برنامج التعاملات الإلكترونية الحكومية (يسر). (العام). تقارير قياس التحول الرقمي الحكومي. [مكان النشر: الرياض، المملكة العربية السعودية].
5. رؤية المملكة 2030. (2016). برنامج التحول الوطني. [جهة النشر].

ثانياً: المراجع باللغة الإنجليزية

1. Al-Harbi, M. A. (2023). *Readiness Assessment of Digital Risk*. [Name], [Volume Number], [Page Range], pp. [Issue Number]. [Journal]
2. Al-Qahtani, S. (2021). *The Impact of Organizational Culture on*. [Name], [Volume Number], [Page Range], pp. [Issue Number]. [Journal]
3. Lee, W & ,Chen, L. (2023). *Assessing Digital Resilience and Sustainability in Government Services*. [Name], [Volume Number], [Page Range], pp. [Issue Number]. [Journal]
4. COSO. (2017). *Enterprise Risk Management—Integrating with Strategy and Performance (COSO ERM Framework)*. Committee of Sponsoring Organizations of the Treadway Commission

- Digital Transformation: The* .(2020) .**Kim, Y & ,Davenport, T. H** .5
.[Publisher Name] .*Seven Imperatives of a Digital Business*
- COBIT 2019 Framework: Governance and* .(2019) .**ISACA** .6
Information Systems Audit and Control .*Management Objectives*
.Association
- Ethical AI Governance and Algorithmic Bias* .(2024) .**Nakamura, T** .7
Volume] ,[Journal Name] .Mitigation in the Public Sector
.[Issue Number]), pp. [Page Range]/Number
- The OECD Digital Government Policy Framework: Six* .(2020) .**OECD** .8
.OECD Publishing .*Dimensions of Digital Government*

الملاحق

السلام عليكم ورحمة الله وبركاته

تحية طيبة وبعد،

طلب تسهيل مهمة جمع بيانات بحث علمي

يشرفنا أن نفيد سعادتك بأن الباحثة امانى سعيد الضويلع، طالبة في جامعة ميد أوشن دراسات عليا بقسم إدارة المخاطر يقوم حالياً بإعداد رسالته العلمية لنيل درجة الماجستير

تتناول الرسالة موضوعاً بالغ الأهمية بعنوان "تطوير إطار منهجي استباقي لإدارة المخاطر الرقمية الناشئة وأثره على استدامة التحول الرقمي في الجهات الحكومية".

ولإتمام المتطلبات المنهجية للرسالة، يتطلب الأمر جمع بيانات ميدانية من قيادات ومختصين لديكم من خلال:

1. توزيع استبانة إلكترونية/ورقية لقياس واقع الممارسات الإدارية للمخاطر الرقمية.

نأمل من سعادتك التكرم بتسهيل مهمة الباحثة وتوجيه من يلزم في الإدارات المعنية (مثل: إدارة المخاطر، الأمن السيبراني، تقنية المعلومات) لتقديم الدعم اللازم لجمع البيانات اللازمة، مع تأكيدنا بأن جميع البيانات والمشاركات سيتم التعامل معها بسرية تامة واستخدامها لأغراض البحث العلمي فقط.

شاكرين ومقدرين تعاونكم المستمر لدعم البحث العلمي وخدمة الأهداف التنموية للمملكة.